Publication des Annales des Mines avec le concours du Conseil général de l'Économie et de l'École de Paris du management

La Gazette DE LA SOCIÉTÉ ET DES TECHNIQUES

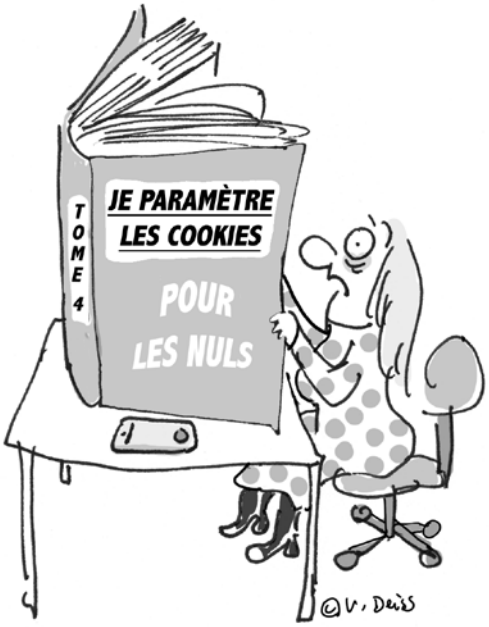
N° 117 · BIMESTRIEL
MAI 2022

« Se défier du ton d'assurance qu'il est si facile de prendre et si dangereux d'écouter »

Charles Coquebert
Journal des mines n°1
Vendémiaire An III (1794)

Vers une protection collective des données personnelles

Savez-vous quel type d'informations vous laissez derrière vous lors de votre navigation internet, à qui vous les laissez et ce qu'ils en ont fait ? Sans doute pas, et c'est normal. Le Règlement général sur la protection des données (RGPD), trois ans après son entrée en vigueur, n'a pas changé la donne. Il n'a pas atteint son plein potentiel et nous proposons des pistes d'amélioration, dans le cadre d'un exercice commun entre le Corps des mines et l'ENA. Plus encore, nous proposons un changement d'approche du RGPD, en le complétant par une dimension collective.



Données personnelles : une collecte d'une ampleur mal connue

Le droit à la protection des données personnelles – se rapportant à une personne identifiée ou identifiable – est garanti par l'article 9 de la Charte des droits fondamentaux de l'Union européenne. Devenu concret après l'entrée en vigueur du RGPD en 2018, il a été largement popularisé par la généralisation des bannières de recueil de consentement.

Malgré cela, l'ampleur de la collecte de données est encore mal comprise par les citoyens. Lors des plus banales actions du quotidien, des données sont collectées et souvent partagées avec plusieurs centaines d'acteurs. On peut le constater en vérifiant la quantité de partenaires que comptent les sites de presse. L'immense majorité de ces acteurs ne sont pas connus de l'utilisateur. Parmi eux, se trouvent des courtiers de données qui recoupent des données provenant de diverses sources pour les revendre ensuite : navigation et achats en ligne, utilisation du smartphone, mais aussi données du monde physique, comme la localisation en temps réel ou les cartes de fidélité de supermarchés.

Un parcours du combattant

En naviguant sur le site lequipe.fr, nous avons fait la connaissance de LiveRamp, une entreprise à laquelle ce site a fourni nos données de navigation. Nous avons donc exercé notre droit d'accès auprès de ce leader du marché des courtiers de données, pour faire la lumière sur nos données. Cette entreprise, que l'usager n'a aucune raison de connaître puisqu'elle ne lui fournit pas directement de service, possédait beaucoup d'informations personnelles assez précises (adresse, âge, revenu, situation conjugale) à notre sujet, pour certaines largement erronées, et les avait revendues à plusieurs entreprises.

LiveRamp a déclaré avoir obtenu ces données auprès d'une entreprise tierce, également inconnue et quasi introuvable sur le web, qui, sollicitée, a affirmé n'être qu'un intermédiaire entre LiveRamp et une troisième entreprise de courtage de données, qui a refusé de confirmer son identité et qui a dû être relancée à plusieurs reprises pour fournir des informations (indirectes) indiquant qu'une quatrième entreprise, également courtier de données, était la source de ces données. Cette entreprise ne nous a répondu que très partiellement et seulement après que la Commission nationale de l'informatique et des libertés (CNIL) a été mobilisée. Par ailleurs, LiveRamp, forte de ses partenariats, collecte également des données sur des sites de e-commerce, d'entreprises comme Carrefour…

Impossible donc, même avec de la patience et de la persévérance, de déterminer l'origine des données et l'ensemble des acteurs à qui elles ont pu être transmises.

Mais pourquoi veut-on mes données ?

La collecte de données vise principalement à alimenter les différents acteurs de la publicité en ligne, qui interagissent à travers ce qu'on appelle la *chaîne programmatique*[1]. Lorsqu'un internaute se connecte à une page web d'un éditeur de contenu, l'ensemble des emplacements disponibles pour afficher des publicités sont mis en vente aux enchères. Les différents annonceurs (ou leur mandataires) placent des enchères en fonction de la valeur qu'ils accordent à chaque client, sur la base des données personnelles qu'ils possèdent sur lui.

La promesse de ce mode d'annonce est de n'afficher des publicités qu'à des clients intéressés et solvables, et ainsi de faire mentir Jon Wanamaker, publicitaire du début du XX^{e} siècle, qui affirmait : « *Je sais que la moitié de mes investissements publicitaires sont en pure perte ; le problème, c'est que je ne sais pas laquelle.* »

La collecte généralisée de données personnelles alimente des craintes chez les citoyens. La première touche à la vie privée, qui pourrait être compromise via la divulgation de certaines données sensibles : sa religion, son orientation sexuelle ou sa présence active sur un site de rencontre.

Les données personnelles peuvent aussi être source de discrimination, volontaire, en restreignant la visibilité d'une annonce à certaines catégories de population par exemple, ou involontaire, à travers les biais des algorithmes.

Les révélations d'Edward Snowden sur les pratiques des services de renseignement américains s'appuyant sur les données des GAFAM, ont accentué les craintes de surveillance étatique, basée sur une collecte massive de données.

Il existe aussi des craintes de manipulation des comportements individuels. Lors de la campagne présidentielle américaine de 2016, l'entreprise Cambridge Analytica a tenté d'influencer le vote d'électeurs en jouant sur l'inférence. Plus largement, les données personnelles alimentent l'existence de "bulles informationnelles" qui enferment les lecteurs du fait des algorithmes de recommandation des réseaux sociaux et qui sont de plus en plus critiquées.

La réponse de la puissance publique

La réponse de la puissance publique s'articule essentiellement autour de deux axes : la politique de la concurrence et le RGPD.

La politique de la concurrence

Les plateformes numériques, dont les plus emblématiques sont issues des GAFAM, concentrent et collectent de grandes quantités de données personnelles. Elles peuvent verrouiller le marché et imposer des conditions de service peu respectueuses des données personnelles à des citoyens captifs.

La volonté européenne de compléter les outils de la concurrence traditionnelle avec des textes permettant une régulation asymétrique de ces plateformes, les *Digital Market Act* et *Digital Services Act*[2], pourraient permettre aux citoyens de choisir un service aux conditions de confidentialité qui leur conviennent. Néanmoins, l'accumulation de données d'utilisateurs par les plateformes constitue un avantage certain sur leurs compétiteurs, et le régulateur de la concurrence pourrait souhaiter les ouvrir davantage pour rétablir un jeu plus égal. Les nouvelles réglementations européennes de la concurrence ne règleront donc pas la question de la protection des données.

Le RGPD

La CNIL a été créée en 1976, à la suite de craintes suscitées par le projet Safari[3]. Au sein de l'Union européenne, le cadre à respecter pour traiter des données personnelles est défini par le RGPD, voté en 2016 et entré en vigueur en 2018.

Ce texte a trois objectifs : assurer la libre circulation des données personnelles au sein de l'Union européenne ; encadrer les pratiques des traitants de données en précisant les six bases légales pour traiter les données personnelles et en prévoyant de grosses sanctions si elles ne sont pas respectées ; et enfin, conférer des droits au citoyen sur ses données. Ce règlement a inspiré des réglementations similaires dans de nombreuses législations, comme celles du Brésil ou de la Californie. Il a aussi largement contribué à la sensibilisation des internautes, en imposant le recueil quasi-systématique de leur consentement via des bannières s'affichant sur les sites internet souhaitant utiliser des cookies.

Souvent présenté comme une réussite, il présente encore deux défauts majeurs : les droits qu'il confère sont peu effectifs en pratique et le consentement est dévoyé[4].

Améliorer la mise en œuvre du RGPD…

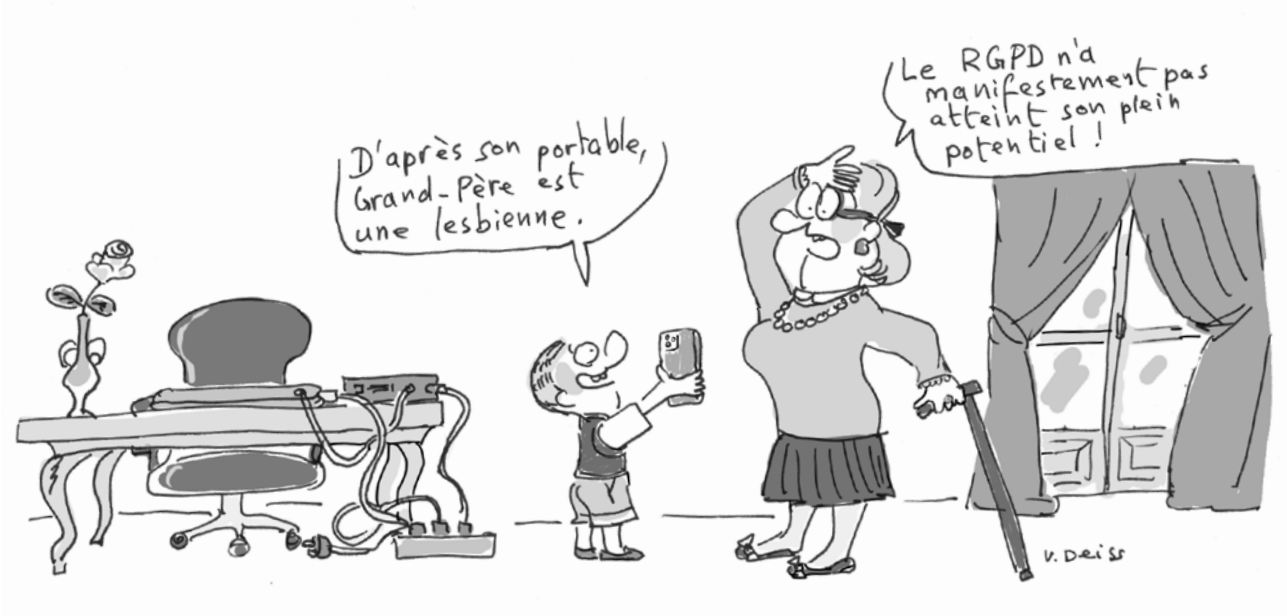
Rendre les droits plus effectifs

Le RGPD confère plusieurs droits au citoyen : le droit d'information sur qui traite ses données, les droits d'accès, de rectification, d'opposition dans certains cas de figure, le droit à la portabilité… Or, nombre d'entre eux ne sont pas réellement effectifs.

Prenons l'exemple du droit d'information : un internaute ne peut pas connaître la totalité des milliers d'acteurs qui manipulent ses données. S'il clique sur "tout accepter", il accepte le partage de ses données avec plusieurs centaines d'acteurs qui ne lui fournissent pas directement de service. S'il souhaite exercer son droit d'accès aux données le concernant, il devra s'adresser individuellement à chacun de ces acteurs. À chaque fois, de nombreuses frictions viendront entraver son expérience utilisateur : contact difficile, réponse lente, incomplète, voire complètement hors sujet, ne précisant ni les destinataires des données ni leurs sources, comme l'a montré notre expérience avec LiveRamp.

Afin d'améliorer l'exercice des droits, nous pensons tout d'abord qu'il est nécessaire, pour les pratiques de la publicité en ligne, de mettre fin au statut de "co-traitants de données personnelles", qui permet à deux acteurs de collecter et traiter les mêmes données sans prendre de responsabilité l'un envers l'autre. S'il se révèle pertinent pour certaines situations, comme l'exploitation des données d'un véhicule autonome, pouvant faire l'objet d'une co-traitance entre le constructeur

« Cette entreprise [...] possédait beaucoup d'informations personnelles assez précises (adresse, âge, revenu, situation conjugale) [...], pour certaines largement erronées, et les a revendues à plusieurs entreprises. »



du véhicule et l'assureur du conducteur par exemple, ce n'est pas le cas pour la publicité en ligne.

Supprimer la possibilité de co-traitance permettrait à l'utilisateur de n'avoir à s'adresser qu'à l'entreprise qui lui fournit un service. En obligeant la formalisation des liens d'échanges de données entre les acteurs, on peut également anticiper une diminution du nombre d'acteurs mobilisés au sein de la chaîne de valeur publicitaire.

Il nous semble aussi nécessaire de renforcer l'exigence de qualité sur ce qui est fourni par les entreprises lors du droit d'accès, notamment afin de permettre la traçabilité des échanges de données. Dans la pratique actuelle, les entreprises n'indiquent ni à qui les données ont été transmises ni d'où elles proviennent, ce qui renforce l'opacité des transactions et ne permet pas de s'assurer qu'aucune donnée obtenue illégalement n'est utilisée.

Enfin, l'amélioration de la coopération entre régulateurs européens est nécessaire pour s'assurer que le traitement des plaintes sera fait avec la même efficacité et dans des délais raisonnables, quel que soit le pays où se trouve l'entreprise mise en cause. Cela pourrait passer par un mécanisme de subsidiarité avec un régulateur européen pour les entreprises les plus structurantes.

Améliorer le consentement

Le consentement est l'une des six bases légales du RGPD pour justifier un traitement de données personnelles, au même titre que l'intérêt légitime ou l'exécution d'un contrat. Or, il nous semble largement dévoyé dans son application actuelle[5].

Il est très pénible pour l'utilisateur, à qui les bannières systématiques imposent des frictions. Il n'est ni libre ni éclairé : les politiques de confidentialité sont excessivement longues et techniques, les interfaces souvent conçues pour biaiser le choix de l'utilisateur, quand le choix qui lui est laissé n'est pas entre les traqueurs et le paiement d'un prix dissuasif pour le service proposé. Parfois, son choix n'est même pas respecté.

Afin d'améliorer l'usage du consentement, les préférences de l'utilisateur pourraient être indiquées une fois pour toutes, par exemple dans les réglages du navigateur, tout en contrôlant le risque de manipulation anticoncurrentielles de la part du fournisseur du navigateur.

Il est également nécessaire que l'alternative au traçage publicitaire ne soit pas payante, en interdisant la pratique du *Cookie Wall*. L'obligation de présenter un design symétrique entre les options d'acceptation et de refus des cookies est déjà présente dans la réglementation, mais très peu respectée : le développement d'outils de détection automatisée des designs inéquitables par la société civile devrait aider le régulateur dans cette tâche.

Enfin, au-delà du choix présenté lors de l'accès à un service internet, l'utilisateur doit toujours pouvoir choisir le service qui lui convient le mieux, y compris du point de vue des conditions de confidentialité.

… ou changer d'approche ?

Le consentement étant si largement dévoyé, on peut s'interroger sur la pertinence de cette approche pour les données personnelles.

Les préférences en matière de protection de la vie privée sont personnelles et peuvent varier d'un individu ou d'une situation à l'autre. Le consentement au partage des données peut paraître à première vue tout à fait adapté pour prendre en compte

la variété des situations et des préférences personnelles, et permettre ainsi à chacun de faire le compromis qui lui convient entre partage et protection de ses données.

Le recours à un consentement individuel occulte le caractère collectif des données personnelles. Le fait, pour un individu, de partager ses données ne fournit pas des informations que sur lui, mais aussi sur les gens avec qui il est en contact ou avec qui il partage des traits communs.

De plus, le consentement intervient dans une relation déséquilibrée entre une entreprise, ayant un intérêt économique ainsi qu'une expertise technique et juridique, et le citoyen. Le recours au consentement individuel en médecine, où le patient donne son accord après que le médecin a exposé les options et les risques, n'empêche pas les autorités sanitaires d'encadrer les pratiques. De même, le droit du travail et les conventions collectives donnent un cadre sans lequel le consentement du travailleur ne peut être accordé.

Dans le cadre du RGPD, cet encadrement global manque et permet aux entreprises de faire consentir les individus à des conditions très défavorables. Les compromis entre partage et protection des données qui émanent ainsi sont plus l'expression d'un rapport de force que d'une préférence individuelle.

Il nous semble que l'approche très individualiste du RGPD gagnerait à être complétée d'une dimension collective : le consentement ex-ante devrait être complété de choix collectifs sur le cadre autorisé des pratiques, et les droits individuels permettant de faire la lumière sur les pratiques ex-post devraient pouvoir être complétés d'une action collective menée par la société civile.

Alors que le développement d'Internet s'est largement basé sur des initiatives citoyennes et des associations, comme W3C, les citoyens ou leurs représentants sont aujourd'hui trop peu associés à sa gouvernance. Une participation accrue de la société civile dans les institutions telles que le Conseil national du numérique (CNNum) et la CNIL, ainsi que dans les plateformes structurantes par le biais de comités de parties prenantes, permettraient aux citoyens d'être davantage associés aux évolutions des conditions générales d'utilisation, aux décisions techniques, mais aussi à la définition de lignes directrices pour la collecte, le traitement et l'usage des données personnelles.

Pour autant, les données personnelles ne doivent pas être exclues du travail démocratique ; elles doivent faire l'objet de commissions parlementaires ad hoc et de consultations citoyennes. Toutes ces solutions nécessitent un portage politique fort, qui aujourd'hui peine à exister malgré les conséquences sur les libertés publiques, la sécurité, ou encore l'accès à l'information.

Par ailleurs, le travail du régulateur doit être prolongé en créant les conditions de la régulation par la société civile. Cela passe par la facilitation de l'exercice des droits individuels et pourrait être complété par l'obligation de permettre l'exportation directe de certaines données, pour faciliter le travail de régulation "par la foule", par des associations de la société civile ou du monde de la recherche. Aujourd'hui, ces travaux sont rendus difficiles, et ceux qui exercent ces fonctions, comme le média The Markup, sont confrontés à la difficulté de l'accès aux données.

L'action de la société civile pourrait aussi être facilitée en renforçant les dispositions de l'action de groupe, qui pourrait être rendue plus facilement accessible. À l'heure actuelle, seules trois associations ont le droit d'ester en justice sur des questions de données personnelles en France !

Conclusion

Alors que la présidence française de l'Union européenne promet de grandes avancées du point de vue de la politique de la concurrence, il n'est pas trop tard pour améliorer la mise en œuvre du RGPD et changer l'approche que nous en avons. Une vision moins individualiste de la protection des données nécessite surtout une prise de conscience collective de ce que la collecte et le traitement massifs de données impliquent pour nos vies quotidiennes autant que pour nos démocraties.

Jean Rérolle et Julia Roussoulières, ingénieurs des mines

NOTES

1 A. Perrot, M. Emmerich, Q. Jagorel, « Publicité en ligne : pour un marché à armes égales », IGF, 2020, disponible en ligne.
2 Voir la « Proposition de règlement du Parlement et du Conseil européen relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques) », décembre 2020.
3 Le projet Safari visait la création d'une base de données centralisant l'ensemble des informations administratives de chaque Français au moyen du numéro INSEE. La révélation de ce projet par *Le Monde* en 1974 fit scandale et conduisit à la création de la CNIL et à l'abandon du projet.
4 Pour de nombreux exemples pernicieux de bannières de recueil de consentement, voir le blog Pixel de tracking ou le rapport du Forbruker Rådet (service norvégien de consultation des consommateurs), « Deceived by design – How tech companies use dark patterns to discourage us from exercising our rights to privacy », 27 juin 2018, disponible en ligne.
5 Le site themarkup.org met notamment en lumière des situations de discrimination liées aux données.

La Gazette de la société et des Techniques

La Gazette de la Société et des Techniques a pour ambition de faire connaître des travaux qui peuvent éclairer l'opinion, sans prendre parti dans les débats politiques et sans être l'expression d'un point de vue officiel. Elle est diffusée par abonnements gratuits. Vous pouvez en demander des exemplaires ou suggérer des noms de personnes que vous estimez bon d'abonner.

Vous pouvez consulter tous les numéros sur le web à l'adresse :
http ://www.annales.org/gazette.html

RENSEIGNEMENTS ADMINISTRATIFS
Dépôt légal Mai 2022

La Gazette de la Société et des Techniques
est éditée par les *Annales des mines*
120, rue de Bercy – télédoc 797 – 75012 Paris
http://www.annales.org/gazette.html
Tél. : 01 42 79 40 84 – Mél. : michel.berry@ecole.org
N° ISSN 1621-2231
Directeur de la publication : François Valérian
Rédacteur en chef : Michel Berry
Illustrations : Véronique Deiss
Réalisation : École de Paris du management
Impression : Graph'Imprim

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA RELANCE
Liberté Égalité Fraternité

l'École de Paris du management