# RGPD, ACTE II

## LA MAÎTRISE COLLECTIVE DE NOS DONNÉES COMME IMPÉRATIF

Jean Rérolle, Julia Roussoulières

THINK-TANK DIGITAL NEW DEAL

*mai 2022*

“

COMME LA PROTECTION DE L'ENVIRONNEMENT, LA PROTECTION DES DONNÉES PERSONNELLES EST UN PROBLÈME COLLECTIF ET DOIT ÊTRE TRAITÉ COMME TEL. "

# SOMMAIRE

**PRÉFACE** ..... 3

**I. UNE COLLECTE DE DONNÉES QUI POSE PROBLÈME**

L'étendue de la collecte, du traitement et du partage de données est mal connue ..... 6
Le moteur de la collecte : le ciblage en ligne ..... 7
En quoi est-ce un problème ? ..... 8

**II. LA RÉPONSE PUBLIQUE : ENTRE POLITIQUE DE LA CONCURRENCE ET ENCADREMENT DES TRAITEMENTS**

La régulation des plateformes ..... 11
L'encadrement des traitements de données personnelles ..... 11

**III. CORRIGER LES DÉFAUTS DU RGPD**

Améliorer l'effectivité des droits ..... 14
Un consentement souvent dévoyé ..... 15
Améliorer le consentement ..... 17

**IV. COMPLÉTER LE RGPD D'UNE APPROCHE COLLECTIVE**

Questionner le consentement individuel ..... 20
Passer de l'individuel au collectif ..... 21

**V. EXEMPLES : QUELS OBJETS POUR LES CHOIX COLLECTIFS ?**

Exemple 1 : Les données d'intérêt général ..... 24
Exemple 2 : La publicité ciblée ..... 25

**CONCLUSION** ..... 28
**NOS PROPOSITIONS** ..... 29

# PRÉFACE

Rarement un règlement de l'Union Européenne aura fait autant débat que le RGPD. Souvent pris comme exemple par certains de la réussite d'un soft power européen jouant enfin le jeu de l'extraterritorialité, symptomatique pour d'autres d'une culture de la régulation contre celle de l'innovation, il constitue pour nous un objet d'étude passionnant.

Quatre ans après sa mise en application, notre think-tank a souhaité publier une note qui remet en perspective le RGPD avec le nouveau package règlementaire européen en cours de validation (DSA, DMA, DGA,...), afin d'imaginer un acte II du RGPD.

Le « Règlement Général sur la Protection des Données » fut en effet chronologiquement, et pas forcément logiquement, le premier règlement à être publié. En étant précurseur et isolé, il a porté seul jusqu'à présent des promesses (comme la portabilité des données ou plus largement la libre circulation des données), créant ainsi un sentiment d'inefficience.

Face à un tel sujet totémique, nous avons décidé d'adopter une approche pragmatique en nous tournant vers des auteurs ayant réalisé un véritable travail d'investigation. Julia Roussoulières et Jean Rérolle ont mené plusieurs mois d'enquête, suivant la piste de leurs données personnelles pour constater que de nombreux droits conférés par le RGPD n'étaient pas effectifs et que le consentement individuel était une approche insuffisante.

Les co-auteurs ont pu démontrer que le rapport de force était totalement déséquilibré entre l'individu et les entreprises demandant le consentement. **L'asymétrie face aux géants numériques et l'opacité entretenue par certains acteurs comme ceux de la publicité en ligne, entravant la bonne exécution du droit.**

Le consentement étant dévoyé, il est donc nécessaire de l'améliorer, et de le rendre plus conforme à ses objectifs initiaux. C'est l'objet des **trois axes de propositions** formulés par les auteurs visant d'une part à améliorer l'effectivité des droits ; d'autre part à rendre le consentement réellement libre et éclairé ; et finalement à mieux articuler les droits individuels avec les actions collectives.

**Arno Pons,**
Digital New Deal

# INTRODUCTION

A mesure que se développent les outils numériques, l'ampleur de la collecte et du traitement des données personnelles ne cesse d'augmenter. Chez certains, cela a nourri des craintes d'intrusion dans la vie privée, par l'Etat ou des acteurs privés, mais aussi de discrimination, de surveillance ou de manipulation.

La réponse réglementaire européenne, le Règlement Général pour la Protection des Données (RGPD), visant à garantir tant la protection des données que leur libre circulation, a été saluée dans le monde entier. Toutefois, la collecte et le partage de données personnelles continuent à se développer, tirés par les besoins de la publicité en ligne, et restent encore d'une ampleur mal comprise par les citoyens. Si le RGPD a sans aucun doute contribué à faire entrer le sujet un peu plus dans le quotidien des internautes européens, il est pour beaucoup le synonyme d'une expérience dégradée, de lourdeurs administratives ou encore d'une boîte noire réglementaire.

**Quatre ans après l'entrée en vigueur du RGPD, nous défendons donc qu'il n'a pas atteint son plein potentiel** pour protéger les citoyens et répondre à leurs attentes : il reste beaucoup à faire !

Nous proposons des pistes pour pallier les dysfonctionnements du RGPD : en améliorant l'expérience utilisateur, et en renforçant le caractère libre et éclairé du consentement. Au-delà des droits individuels qu'il confère, **nous proposons de le compléter par la possibilité d'actions collectives, en associant davantage la société civile, et de mieux articuler consentement individuel et choix collectifs.**

Les données personnelles sont un sujet politique. C'est en l'acceptant que nous pourrons construire un avenir plus souhaitable pour la maîtrise de nos données personnelles.

LA MASSE DE DONNÉES TRÈS PRÉCISES COLLECTÉES PAR DES SOCIÉTÉS PRIVÉES, AINSI QUE LEUR POUVOIR PRÉDICTIF, OUVRE LA POSSIBILITÉ DE LEUR UTILISATION PAR DES ETATS OU DES GROUPES MALVEILLANTS "

# I. UNE COLLECTE DE DONNÉES QUI POSE PROBLÈME

En 2020, 90 % des Français se sont connectés à internet. 80 % d'entre eux l'ont fait quotidiennement[1]. Parmi ces internautes, 72 % ont utilisé un réseau social, et 70 % ont effectué des achats en ligne. Ce faisant, ils ont partagé avec des acteurs privés une grande quantité de données que l'on peut qualifier de personnelles.

### QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

La CNIL, Commission Nationale de l'Informatique et des Libertés, définit les données personnelles de la manière suivante : *« Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. »*

Les données personnelles peuvent être de nature différente. Certaines **données personnelles sont volontairement et consciemment partagées** par l'utilisateur avec un site à travers des formulaires et des abonnements : le nom, le prénom, la date de naissance, etc. D'autres sont partagées de façon moins aisément perceptible par l'internaute: ce sont des **données observées**, notamment par le biais des cookies, et qui constituent des traces numériques.

De ces **données peuvent être inférées** des informations sur les individus : âge, niveau de revenu, structure familiale, préférences politiques… Ces informations peuvent ensuite être retravaillées, partagées, exploitées, pour entraîner des algorithmes de recommandation ou de prédiction.

### QU'EST-CE QU'UN COOKIE ?

Un cookie est un petit fichier informatique enregistré sur un appareil durant la navigation en ligne, qui permet l'identification et le suivi d'un internaute. Les cookies peuvent contenir de nombreuses données observées, comme des informations sur votre navigateur, votre lieu de connexion, ou encore la dernière fois que vous vous êtes rendu sur tel ou tel site.

## L'ÉTENDUE DE LA COLLECTE, DU TRAITEMENT ET DU PARTAGE DE DONNÉES EST MAL CONNUE

Si les bannières de recueil de consentement systématique (où l'on demande à l'utilisateur d'accepter ou refuser les cookies) ont rendu visible le suivi de la navigation en ligne, **le périmètre de la collecte et la quantité d'acteurs impliqués sont en général méconnus des internautes**. En effet, cette collecte peut aller de simples cookies à la localisation précise et continue de l'utilisateur, alors que le nombre d'acteurs collectant des données sur un simple site de presse peut aller jusqu'à plusieurs centaines[2].

**Par exemple, dans le domaine des applications mobiles,** une étude de l'association de consommateur norvégienne Forbruker Radet[3] a mis en lumière la collecte et le partage massif de données opéré par les applications sur smartphone des utilisateurs.

L'association a analysé les flux de données émis par 10 applications, et leurs destinataires. Cela a permis de vérifier que l'application de rencontre LGBT+ Grindr collecte puis partage l'identité de ses utilisateurs ainsi que des données de localisation ou des préférences sexuelles précises avec une vingtaine de partenaires publicitaires, sans que l'utilisateur

[1] *Référentiel des usages numériques, Février 2021, CSA-ARCEP, En ligne.*
[2] *Par exemple 700 sur www.lefigaro.fr, ou encore 426 pour le site www.lequipe.fr.*
[3] *Out of controll, Forbruker Radet, 01/2020, en ligne*

en soit clairement informé ou qu'il puisse s'y opposer. Il en va de même pour l'application Muslim Assistant, qui partage la localisation et l'identité de ses utilisateurs à de nombreux partenaires. Dans ces deux cas, le fait d'être utilisateur de l'application est une donnée personnelle sensible car cela révèle des informations sur la religion ou l'orientation sexuelle. Grindr a été condamnée à 10 millions d'euros d'amende par l'autorité de protection des données personnelles norvégienne suite à cette enquête[4].

**Les données personnelles ainsi collectées par des applications ou des sites internet sont partagées avec d'autres entreprises :** partenaires publicitaires, entreprises technologiques, mais aussi entreprises du monde « physique », bien loin des seules GAFAM , souvent seules décriées pour leur gestion des données. Souvent, ces données passent aussi entre les mains d'intermédiaires moins connus du grand public, les *data brokers* ou courtiers en données.

Ces *data brokers* fondent leurs modèles d'affaires sur la revente et le partage de données collectées auprès de sources variées. L'un d'entre eux, LiveRamp, est ainsi le partenaire de sites de presse comme Le Monde, Le Figaro, L'Équipe ou encore d'acteurs de la distribution comme Carrefour. La lecture d'un article ou l'acte d'achat par un individu sont autant d'informations que LiveRamp peut ensuite partager avec ses partenaires sans que l'individu concerné n'en soit informé.

## LE MOTEUR DE LA COLLECTE : LE CIBLAGE EN LIGNE

Le marché de la publicité en ligne est le principal consommateur de données personnelles. Cela tient notamment au mécanisme de la publicité programmatique utilisé pour affecter une annonce à un internaute. Ce marché finance la plupart des services numériques, qui sont de ce fait gratuits pour l'utilisateur.

Au début du XX$^{e}$ siècle, le publicitaire Jon Wanamaker disait : *« Je sais que la moitié de mes investissements publicitaires est dépensée en pure perte ; le problème, c'est que je ne sais pas laquelle »*. La promesse de la publicité ciblée individualisée est de se débarrasser de cette moitié non productive des dépenses publicitaires en ne visant que des clients dont l'intérêt potentiel pour le produit est connu au préalable.

### LA CHAÎNE PROGRAMMATIQUE DE LA PUBLICITÉ EN LIGNE

Lorsque l'utilisateur se connecte à une page sur le site d'un éditeur, une enchère est organisée pour avoir le droit d'afficher une publicité dans les différents espaces possibles sur la page web. Chaque annonceur potentiel place une enchère, en fonction de la valeur qu'il accorde à l'utilisateur. L'annonceur estime cette valeur en fonction des informations qu'il détient sur l'utilisateur. Plus il possède de données, plus il estime avec justesse l'enchère à placer, c'est pourquoi il peut parfois acheter des données supplémentaires à un courtier de données, comme LiveRamp. De très nombreuses entreprises sont spécialisées sur les différentes étapes du processus publicitaire, formant un écosystème appelé *AdTech*.

[4] *20 minutes, En Norvège, Grindr pourrait payer cher, 2020, en ligne.*


*Figure 1 : Les acteurs de la publicité en ligne.*

*Source : Autorité de la Concurrence.*

L'utilisateur ne perçoit qu'une infime partie du chemin que parcourent ses données personnelles.Elles permettent notamment de proposer des **recommandations de produits individualisées**, ou d'estimer le prix qu'un client est prêt à payer pour un produit, et donc s'il est pertinent de lui proposer ou non une réduction sur le prix : c'est une forme de **discrimination par les prix**. Pour l'utilisateur, les données de sortie de ces algorithmes, c'est-à-dire les publicités qu'il voit, les produits qui lui sont recommandés et les prix qui lui sont proposés sont la seule manifestation de l'usage généralisé de ses données qui est faite par les différents acteurs numériques.

## EN QUOI EST-CE UN PROBLÈME ?

Ces manifestations de l'usage des données n'éclairent pas l'utilisateur sur l'étendue de la collecte et du partage de ses données. Cette méconnaissance du périmètre et des acteurs partageant des données de nature très diverse alimente un grand nombre de craintes.

D'abord, certains craignent pour la **protection de leur vie privée**, ne souhaitant par exemple pas que des informations confidentielles ou compromettantes à leur égard soient divulguées. Dans le cas de l'étude menée par l'association de consommateur norvégienne Forbruker Radet[5], cette crainte est renforcée par la sensibilité des informations détenues par les applications étudiées (orientation sexuelle, religion).

Ensuite, les craintes concernent les possibilités de **discrimination** offertes par la connaissance de données personnelles. L'opacité de certains algorithmes ne facilite pas la mise en lumière de ces phénomènes, et de nombreux travaux de recherche ont d'ores et déjà montré des cas de discrimination **volontaire** - Facebook a notamment été poursuivi par le ministère du Logement américain pour avoir permis aux annonceurs de limiter la visibilité d'offres de logement aux personnes d'une certaine origine[6] - et de discrimination **involontaire** causée par les biais dans la structure même des algorithmes[7].

Puis, les craintes d'une nouvelle forme de **surveillance** émergent. Les révélations d'Edward Snowden avaient, dès 2013, révélé les moyens mis en oeuvre par l'Etat américain pour surveiller ses ressortissants[8]. La masse de données très précises collectées aujourd'hui par des sociétés privées, ainsi que leur pouvoir prédictif, ouvre la possibilité de leur utilisation par des Etats ou des groupes malveillants - ainsi, l'Etat américain a-t-il acheté à des sociétés privées des bases de données de géolocalisation pour surveiller ses frontières[9].

[5] *Out of controll, Forbruker Radet, 01/2020, en ligne*
[6] *Facebook poursuivi pour discrimination par le ministère du logement américain, Les Echos, 2019, en ligne.*
[7] *« Algorithmes : prévenir l'automatisation des discriminations », Défenseur des droits, 2020, en ligne.*
[8] *https://www.lemonde.fr/pixels/article/2019/09/13/ce-que-les-revelations-snowden-ont-change-depuis-2013_5509864_4408996.html*
[9] *Federal agencies use cellphone Location Data for Immigration Enforcement, The Wall Street Journal, 2020, en ligne.*

Enfin, cette manne d'informations individuelles peut être utilisée à des fins de **manipulation**. Le pouvoir de prédiction accordé par la connaissance très fine des internautes[10] accorde aux plus grandes entreprises du numérique un « pouvoir d'instrumentation » qui leur permet d'influencer les comportements des individus. Si cette influence se manifeste pour le moment surtout sur des comportements d'achat, le scandale Cambridge Analytica et les fantasmes qui lui ont été associés laissent imaginer les utilisations politiques et sociales qui pourraient être faites de la connaissance des individus. La publicité en ligne et les algorithmes de recommandation, par leur personnalisation à l'extrême, permettent d'ores et déjà de véhiculer des messages adaptés à une audience et de « bulles informationnelles »[11].

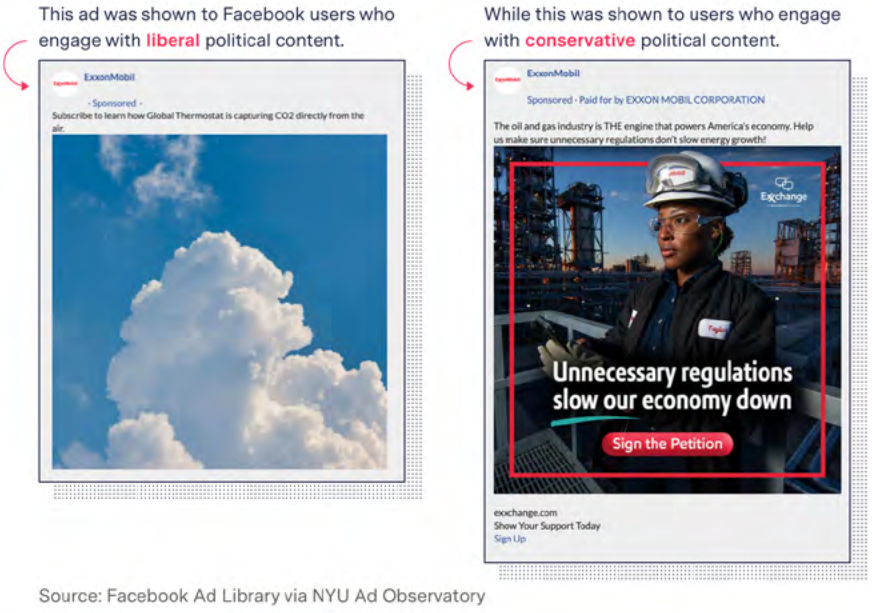


*Figure 2 : ExxonMobil montre des publicités bien différentes à des cibles aux sensibilités politiques opposées.*

*Source : The Markup.*

[10] *Voir le livre de la juriste et professeur de droit à Harvard : Zuboff, S., L'âge du capitalisme de surveillance, 2020.*
[11] *How Facebook's ad system lets company talk out both sides of their mouths, The Markup, 2021, en ligne.*

LE RGPD ATTEINDRA
SON PLEIN POTENTIEL
SI NOUS CORRIGEONS
SES DÉFAUTS ET SURTOUT
SI NOUS ALLONS
PLUS LOIN AVEC UNE
APPROCHE COLLECTIVE
DES DONNÉES "

# II. LA RÉPONSE PUBLIQUE : ENTRE POLITIQUE DE LA CONCURRENCE ET ENCADREMENT DES TRAITEMENTS

L'action publique mobilise deux principaux leviers pour permettre la protection des données personnelles : l'encadrement des traitements de données personnelles et les outils de politique de la concurrence. L'actualité se concentre sur les nouveaux outils de la politique de la concurrence, mais le RGPD a-t-il dit son dernier mot ?

## LA RÉGULATION DES PLATEFORMES

Les plateformes numériques, dont les plus emblématiques sont issues des GAFAM (Google, Amazon, Facebook, Apple et Microsoft) américaines, concentrent et collectent de grandes quantités de données personnelles. Par leurs positions dominantes, elles verrouillent le marché et peuvent fixer leurs conditions de service en termes de respect des données personnelles à des citoyens captifs.

Face aux limites de la politique de la concurrence traditionnelle, l'Union Européenne a décidé de se doter de nouveaux textes, permettant une régulation asymétrique des plateformes dites « structurantes », afin d'en limiter le pouvoir de marché. Ces textes européens sont notamment le Digital Markets Act (DMA) et le Digital Services Act (DSA) et constituent un véritable changement de paradigme pour la politique de la concurrence européenne, qu'il conviendra d'évaluer dans les prochaines années.

Le renforcement de la concurrence peut avoir des effets positifs pour la protection des données personnelles en permettant au citoyen de choisir un service donc les conditions de confidentialité lui conviennent. A l'inverse, protection des données et régulation de la concurrence peuvent s'opposer : les données d'utilisateurs accumulées confèrent un avantage concurrentiel à l'entreprise en leur possession, et l'autorité de la concurrence pourrait vouloir contraindre l'entreprise à en autoriser l'accès à la concurrence. Dès lors, des décisions renforçant la protection des données peuvent avoir des conséquences anticoncurrentielles fortes[12].

**Néanmoins, les interactions entre concurrence et protection des données sont trop complexes pour que la politique de la concurrence soit la seule arme employée à cet effet**[13].

## L'ENCADREMENT DES TRAITEMENTS DE DONNÉES PERSONNELLES

La CNIL est créée en France en 1976 suite à des craintes de surveillance des Français suscitées par le projet Safari[14]. Elle est depuis lors une autorité administrative indépendante chargée de faire appliquer les lois relatives à la protection des données personnelles.

L'article 8 de la charte des droits fondamentaux européens garantit à tout citoyen européen le droit à la protection de ses données personnelles. Ces droits et les règles à suivre en matière de protection des données personnelles dans l'Union européenne sont principalement définies

[12] *Le projet de Privacy Sandbox de Google Chrome, censé améliorer la protection de la vie privée sur le navigateur, a des conséquences potentiellement importantes sur les acteurs de la publicité en ligne. Voir Gérardin D., Google as a de facto Privacy Regulator: Analyzing Chrome's Removal of Third-party Cookies from an Antitrust Perspective, TILEC Discussion Paper, 2020, en ligne.*

[13] *Tucker, C., Marthews A., Privacy policy and competition, Economic Studies at Brookings, 2019, en ligne.*

[14] *Le projet Safari de création d'un grand fichier administratif référençant l'ensemble des Français via leur numéro INSEE avait suscité à l'époque une grande opposition, notamment dans un célèbre article :Safari ou la chasse aux Français, Le Monde, 1974.*

dans le Règlement Général pour la Protection des données personnelles, le RGPD. Voté en 2016, entré en vigueur en 2018, le RGPD est fondé sur trois objectifs.

Le premier est d'assurer la libre circulation des données dans l'espace économique européen.

Le deuxième est d'encadrer les pratiques des traitants de données, notamment les entreprises opérant en Europe, en précisant les fondements juridiques selon lesquelles une entité peut traiter des données et les précautions qu'elle doit prendre en fonction du risque que constitue le traitement de données. Le recueil du consentement de l'utilisateur, et qui constitue une des six bases légales de traitement, doit être **explicite, libre et éclairé** et est encadré plus strictement, donnant naissance aux bannières porteuses du bouton « accepter les cookies »sur les sites internet. Pour les contrevenants, le texte prévoit des amendes allant jusqu'à 50 millions d'euros ou 4% du chiffre d'affaires mondial, bien plus élevées que ce qui était possible auparavant.

Enfin, le troisième objectif est de garantir au citoyen des droits inaliénables sur ses données, tels que le droit d'information sur qui traite ses données, le droit d'accès, de rectification, d'opposition dans certains cas de figure, le droit à la portabilité, etc…[15]

Ce règlement a connu une influence mondiale et a été décliné sous des formes plus ou moins proches dans divers pays ou régions, de la Californie au Brésil. Il est pour cette raison notamment souvent présenté comme un succès pour l'influence européenne sur la scène internationale.

Le RGPD a contribué à la sensibilisation des internautes au sujet des données personnelles : en 2019, et après la grande campagne médiatique qui accompagna son entrée en vigueur, 70% d'entre eux déclarent y être plus sensibles qu'auparavant[16]. En réalité, et du point de vue de l'expérience quotidienne du citoyen, l'influence du RGPD s'est surtout manifestée via les bannières de recueil de consentement devenues obligatoires sur tous les sites internet souhaitant utiliser les cookies.

Alors que le Digital Markets Act s'apprête à entrer en vigueur, il est donc temps de s'intéresser à nouveau au RGPD. **Pour nous, il n'a pas atteint son plein potentiel car il a deux défauts majeurs.**

**D'une part, les droits conférés par le RGPD ne sont aujourd'hui pas tous effectifs**. En effet, malgré le droit d'information, aucun internaute ne peut prétendre connaître la totalité des acteurs en possession de ses données. Sans connaître la totalité des acteurs, il ne peut pas non plus connaître la totalité des données qui s'échangent sur lui. Exercer son droit d'accès est souvent fastidieux et nécessite de s'armer de patience et courage. L'expérience utilisateur de l'exercice des droits est sans commune mesure avec les standards habituels des services numériques.

**D'autre part, la notion de consentement est dévoyée**, n'étant que rarement conforme aux exigences du RGPD car ni libre, ni éclairé, et de surcroît son expérience est désagréable pour l'utilisateur. De plus, le consentement seul ne suffit pas à répondre à toutes les situations de partage de données. Le recours à l'intérêt légitime est lui aussi flou et source d'abus, et mériterait d'être précisé.

Nous proposons dans un premier temps de **corriger ces défauts par une meilleure mise en œuvre** du RGPD, et dans un second temps d'aller plus loin encore avec une **approche collective des données**. C'est ainsi que le RGPD atteindra son plein potentiel.

[15] *Règlement (UE) 2016/679 du 27 avril 2016 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, en ligne.*
[16] *Sondage IFOP réalisé en avril 2019 sur un échantillon représentatif de 1 000 personnes, en ligne.*

“

METTRE FIN AU STATUT DE “CO-TRAITANTS DE DONNÉES PERSONNELLES” POUR LES PRATIQUES DE LA PUBLICITÉ EN LIGNE ”

# III. CORRIGER LES DÉFAUTS DU RGPD

## AMÉLIORER L'EFFECTIVITÉ DES DROITS

Illustrons les difficultés d'exercice des droits à l'aide d'un exemple concret. Nous avons voulu vérifier par nous mêmes si un *data broker* parmi d'autres, LiveRamp, détenait des informations sur nous : nous avons donc exercé notre droit d'accès, conféré par le RGPD, auprès de cette société. Concrètement, il faut envoyer un mail avec sa requête et une pièce d'identité, et patienter 3 semaines.

LiveRamp, société que l'utilisateur moyen ne connaît pas étant donné qu'elle ne lui fournit pas directement de service, possède effectivement de nombreuses données sur l'un d'entre nous (nom, adresse, numéro de téléphone) et a inféré un certain nombre d'informations (âge, niveau de revenus, situation familiale), parfois erronées. La source de ces données n'est pas indiquée. Seule la provenance de l'adresse postale est indiquée, une société du nom d'IG Conseil, également inconnue de l'utilisateur. Aucun contact de cette société n'est disponible en ligne, il est donc nécessaire d'interroger LiveRamp pour obtenir un contact.

Joint, IG Conseil indique n'être qu'un intermédiaire entre LiveRamp et une troisième société non nommée, mais dont l'e-mail fourni révèle qu'elle est Cap Décision, PME du Val d'Oise. Interrogée à son tour sur l'origine des données, cette société se borne à répondre qu'elles ont été supprimées, ce qui n'est pas l'objet de la demande. La capture d'écran fournie semble indiquer que la source des données est une entreprise du nom d'Edentify, propriétaire du site Focus-news.fr. Contactée, cette entreprise n'a pas répondu. Une plainte à la CNIL a été déposée. Nous savons que ces données sont issues de l'opérateur de téléphonie free, mais nous ne savons pas par quelles mains elles ont transité avant d'arriver chez Edentify. Parallèlement, nous avons découvert que la société de vente de numéros de téléphone SOS Fichiers, détenait aussi des informations sur nous dont la provenance n'était autre que… CapDécision. Le chemin parcouru par nos données est retracé Figure 3.

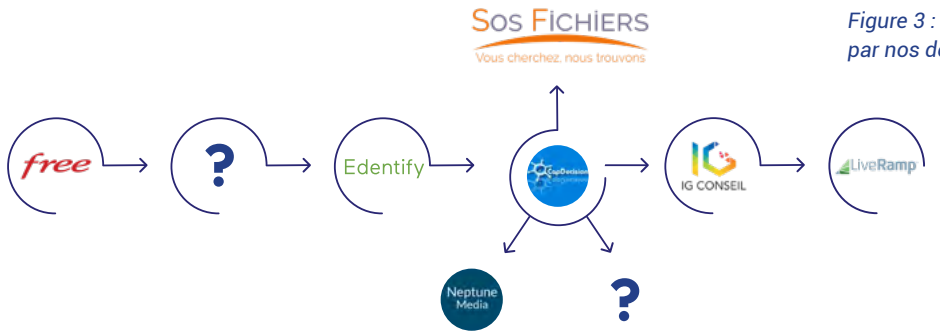


*Figure 3 : Le chemin parcouru par nos données*

De nombreuses frictions entravent l'expérience de l'utilisateur lors de l'exercice de ses droits. Ceux-ci sont pourtant essentiels car ils ont le potentiel pour convaincre l'utilisateur de la confiance qu'il doit accorder à un service, et qu'ils peuvent permettre à la société civile de faire la lumière sur les pratiques des entreprises.

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

Dans le cadre de la publicité en ligne, ce cadre légal nous semble par contre tout à fait dévoyé : les fournisseurs de services à l'utilisateur (typiquement, l'éditeur de presse) associent leurs propres fournisseurs de services publicitaires comme des co-traitants de données (désignés comme "partenaires" dans les politiques de confidentialité), et non comme des sous-traitants. En conséquence, pour exercer le droit d'accès à ses données, l'utilisateur doit s'adresser à la totalité des co-traitants : en règle générale, plusieurs centaines. Il lui est donc impossible en pratique de savoir qui traite ses données - potentiellement plusieurs centaines d'acteurs à chaque article lu- et plus encore d'y accéder.

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, seule qu'il est réellement en mesure de connaître, pour l'exercice de ses droits. En obligeant la formalisation des liens d'échanges de données entre les acteurs et les responsabilités respectives, on peut également anticiper une diminution du nombre d'acteurs mobilisés au sein de la supply chain publicitaire. A l'heure actuelle, les régies publicitaires des grands médias indiquent ne connaître qu'une centaine d'acteurs parmi le demi-millier qui sont listés comme "partenaires". L'absence de risque juridique à ajouter des partenaires en tant que co-traitants alimente l'inflation du nombre d'entreprises collectant des données personnelles.

Il nous semble aussi nécessaire de renforcer l'exigence de qualité sur les éléments fournis 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 pas à qui les données ont été transmises, ni d'où elles proviennent, renforçant un sentiment d'opacité sur les transactions, et ne permettant pas de s'assurer qu'aucune donnée obtenue illégalement n'est utilisée.

L'expérience utilisateur de l'exercice des droits pourrait être améliorée en s'inspirant de l'outil Signal Conso mis en place par la DGCCRF pour les plaintes de consommateur concernant des non-conformités de produits. Les échanges en citoyen et entreprises s'y déroulent sous l'égide du régulateur, ce qui permet une intervention rapide en cas de litige, et limite drastiquement le nombre de cas où une plainte est effectivement nécessaire au citoyen pour obtenir gain de cause.

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 l'entreprise qui traite les données ait choisi de se domicilier. Cela pourrait passer par un éventuel mécanisme de subsidiarité avec un régulateur européen pour les entreprises les plus structurantes en matière de gestion des données personnelles.

## UN CONSENTEMENT SOUVENT DÉVOYÉ

Le RGPD renforce la notion de **consentement**, déjà introduite dans Loi Informatique et Libertés, en la définissant ainsi dans son article 4 : *« toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».*

L'article 6 du RGPD reconnaît le consentement comme l'une des six bases légales de traitement de données, en parallèle de l'intérêt légitime, de l'intérêt public ou encore de l'exécution d'un contrat.

[17] *"Après la crise, les communs numériques en quête de reconnaissance", Claire Legros, Le Monde, 31 juillet 2020.*

**Aujourd'hui, le consentement nous paraît dévoyé pour plusieurs raisons.**

**L'expérience utilisateur est mauvaise.** L'expérience quotidienne des bannières intempestives demandant à l'utilisateur sont à l'origine d'un agacement. Les utilisateurs expriment une certaine lassitude. Cette « fatigue du consentement » amène même certains internautes à installer des outils automatisés acceptant l'ensemble des cookies[17].

**Le consentement n'est ni libre, ni éclairé.** Les Conditions Générales d'Utilisation (CGU) sont longues (la lecture exhaustive de toutes les CGU auxquelles un internaute moyen est exposé prendrait 76h par an[18]) et comportent une terminologie technique qui nuisent à leur lecture et leur bonne compréhension par les utilisateurs.

Par ailleurs, les interfaces sont souvent construites de manière à pousser l'internaute à accepter les CGU, notamment via des interfaces aux designs trompeurs ou manipulateurs. C'est ce qu'on appelle les dark patterns : ces pratiques ne sont pas formellement interdites, mais peuvent aller à l'encontre d'un consentement libre et éclairé[19].


*Figure 4 : Un exemple de dark pattern.*

**L'utilisateur n'a pas le choix**

La liberté du consentement est aussi condition de l'existence d'un véritable choix[20]. L'accès à certains services peut être conditionné au partage de données alors que l'utilisateur n'a d'autre alternative : cela peut être le cas pour les plateformes numériques structurantes mais aussi quand le service est un site de presse et que la lecture d'un article ne peut se faire sur un autre site.

Une étape supplémentaire a été franchie avec l'apparition des *cookies walls*, ou murs de traceurs. Cette fois, l'utilisateur se voit proposer deux alternatives : soit il accepte les conditions de partage de ses données, soit il paie pour le service. Cette solution, très courante sur les sites de presse en ligne, n'est pas non plus illégale. Même si la CNIL a souhaité l'interdire via ses lignes directrices[21], le Conseil d'Etat a jugé que la licéité de cette pratique devait être décidée au cas par cas : *« la liberté du consentement des personnes doit être appréciée au cas par cas, en tenant compte notamment de l'existence d'alternatives réelles et satisfaisantes proposées en cas de refus des cookies. »*


*Figure 5 : Un exemple de cookie wall.*

*Source : Capture d'écran du site Marmiton.fr.*

[17] *Comme par exemple l'extension de navigateur I don't care about cookies, en ligne.*
[18] *A. McDonald et al., « The Cost of Reading Privacy Policies », A Journal of Law and Policy, 4 /3, 2008, p. 543-568, en ligne.*
[19] *Une étude sur les bannières de consentement de 10 000 sites a ainsi démontré que seules 11,8 % d'entre elles étaient conformes au RGPD car remplissant trois critères cumulatifs : (i) le caractère explicite du consentement, par exemple via la présence d'un bouton ; (ii) l'égale simplicité entre « tout accepter » et « tout refuser » ; (iii) l'absence de case pré-cochée en faveur du consentement. Voir M. Nouwens et al., « Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence », Conference on Human Factors in Computing Systems, 8 janvier 2020, en ligne.*
[20] *Le considérant 42 du RGPD l'exprime : « Le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice. »*
[21] *Les inquiétudes de la CNIL au sujet des cookie walls, notamment sur la monétisation et ses risques, sont très bien résumées dans un article du régulateur, en ligne.*

Qu'il soit conforme ou non, **le consentement n'est parfois pas du tout respecté.** En effet, certains sites se permettent de partager les données de leurs visiteurs avant même que ceux-ci n'aient consenti ou non, d'autres partagent les données malgré le consentement[22].

## AMÉLIORER LE CONSENTEMENT

# CONSIDÉRANT QUE LE CONSENTEMENT EST AUJOURD'HUI DÉVOYÉ, IL EST NÉCESSAIRE DE L'AMÉLIORER ET DE LE RENDRE PLUS CONFORME À SES OBJECTIFS INITIAUX.

### EN AMÉLIORANT L'EXPÉRIENCE UTILISATEUR

Plutôt que de systématiser l'acceptation ou le refus des cookies, il est possible d'agir sur l'expérience utilisateur. Par exemple, le futur règlement « vie privée et communications électroniques » (ePrivacy) prévoit de centraliser le paramétrage des préférences en matière de consentement directement sur le navigateur. Cette décision pose de nombreuses questions de concurrence, et a d'ailleurs été combattue par les éditeurs. Ceux-ci souhaitent garder un lien direct avec leurs clients et craignent que la configuration du navigateur soit biaisée par Google et Apple, qui représentent 90 % du marché, par exemple en nudgant les utilisateurs pour qu'ils acceptent le suivi de Google et pas des autres entreprises. Afin d'éviter cette situation, nous recommandons que le navigateur soit inscrit dans le champ des plateformes structurantes du DMA et du DSA, et qu'ainsi le régulateur puisse s'opposer à une modification technique anti-concurrentielle.


*Figure 6 : Elon Musk en a rêvé, l'Europe l'a fait.*
*Source : Twitter*

[22] *C'est ce que montre Pixel de Tracking dans un article riche en mauvais exemples, en ligne.*

### EN LE RENDANT PLUS LIBRE ET PLUS ÉCLAIRÉ :

La CNIL a voulu, via de nouvelles lignes directrices entrées en vigueur en avril 2021, rendre ces designs plus équilibrés, selon le principe de la Figure 6. Ce modeste changement, quoiqu'encore peu respecté, bouleverse à lui seul le taux de consentement : le Syndicat des Régies Internet (SRI) estime qu'il entraîne une chute du consentement entre 30 et 60 points.

Ces nouvelles lignes directrices et la prolifération de designs trompeurs nécessitent de poursuivre le renforcement des compétences au sein des organes de régulation en la matière, ainsi que de les doter d'outils automatisés de détection de designs abusifs.

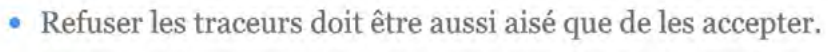


*Figure 7 : Les nouvelles lignes directrices de la CNIL.*
*Source : CNIL*

L'association NOYB se montre pilote en la matière et a annoncé avoir déposé plus de 500 mises en demeure à des sites ne respectant pas les lignes directrices de la CNIL, en s'appuyant sur un outil automatisé de détection similaire à celui ci.[23]

Afin d'éclairer le choix des utilisateurs, il nous semble aussi impératif de poursuivre la sensibilisation et la bonne information des citoyens sur les enjeux de données personnelles. La méconnaissance de l'étendue de la collecte et du partage des données n'est pas une fatalité, et il nous semble essentiel de développer une culture de la donnée. Plusieurs pistes sont envisageables pour améliorer l'information et renforcer les dispositifs de formation ou les campagnes de communication, notamment via les dispositifs de sensibilisation au numérique à l'école comme l'initiative Pix.

### EN DONNANT LE CHOIX

Dans l'espace numérique, le citoyen est souvent captif de services bénéficiant de forts effets de réseaux et donc de monopoles naturels, qui peuvent à ce titre fixer leurs conditions de service, y compris en termes de politique de confidentialité. Pour permettre au citoyen de choisir des services qui lui conviennent, on peut envisager diverses actions visant à faire émerger des alternatives.

Le droit à la portabilité, inscrit dans le RGPD, peine à être mobilisé en pratique en raison de nombreux freins. Les standards communs internationaux manquent pour permettre des échanges fluides, et les initiatives telles que Gaïa-X (en Europe) ou le Data free-flow with Trust (mené par le Japon) sont nécessaires et doivent être soutenues. Pour inciter le citoyen à utiliser son droit à la portabilité, on peut le nudger le en mettant en place un "Blue button" permettant l'export de ses données, à l'instar de ce qui avait été mis en place par l'administration Obama pour les données de santé.

Enfin, le soutien public à l'écosystème innovant des "tiers de confiance", qui visent à fluidifier l'expérience utilisateur du changement de service et la réutilisation des données, pourrait être renforcé. Divers leviers pourraient être utilisés comme la facilitation de leur inclusion dans les commandes publiques, le renforcement et la généralisation de leurs partenariats avec les acteurs locaux et l'autorisation de récupération de données par des méthodes de *scraping* dans le cadre du Data Governance Act.

[23] *https://www.lemonde.fr/pixels/article/2021/05/31/cookies-sur-internet-des-militants-a-l-offensive-cont re-la-terreur-des-traceurs-informatiques_6082155_4408996.html*

LE RAPPORT DE FORCE EST DÉSÉQUILIBRÉ ENTRE L'INDIVIDU ET LES ENTREPRISES DEMANDANT LE CONSENTEMENT "

# IV. COMPLÉTER LE RGPD D'UNE APPROCHE COLLECTIVE

## QUESTIONNER LE CONSENTEMENT INDIVIDUEL

Le consentement est facilement dévoyé, et malgré les opportunités identifiées pour l'améliorer, il convient de s'interroger sur la pertinence de ce concept dans le domaine du ciblage publicitaire.

### D'ABORD, POURQUOI AVOIR RECOURS AU CONSENTEMENT ?

La notion de *privacy*, que l'on peut schématiquement traduire en français par « vie privée », est complexe[24] et contextuelle[25] : elle n'engage pas les mêmes notions pour des individus différents, et peut s'exprimer différemment selon la situation. Classiquement, le droit au respect de la vie privée a été défini comme un « droit à être laissé tranquille »[26] et sans intrusion dans sa sphère intime. La notion a évolué pour englober aussi l'idée d'autodétermination informationnelle : chaque individu est libre de choisir ce qu'il veut révéler ou non, faisant de la vie privée « un compromis entre la protection et le partage des données personnelles[27] ».

Le consentement est, à première vue, une réponse adaptée à cette complexité et l'exigence de liberté de la personne en matière d'usage de ses données personnelles : on demande à chaque individu d'accepter ou de refuser une situation en fonction de ses intérêts individuels et contextuels. Par là, on accepte qu'il consente parfois à une situation juridique susceptible de lui causer un préjudice.

Le consentement n'est pas une notion propre aux données et à la protection de la vie privée. Il est aussi mobilisé dans la relation médicale : au nom de la préservation de l'intégrité du corps, il convient au médecin d'informer son patient sur les risques et d'obtenir son consentement en vue d'un acte médical.

### MAIS CETTE APPROCHE PRÉSENTE SES LIMITES

**Le consentement,** tel qu'il se présente aujourd'hui à l'internaute, n'est **ni agréable, ni libre, ni éclairé**, nous l'avons montré. Il fait peser sur l'individu seul le poids d'un arbitrage ex ante alors qu'il n'a qu'une information limitée sur l'étendue de la collecte ou sur les utilisations qui sont faites de ses données, sans réel choix et informations. L'améliorer via les propositions que nous avons déjà formulées est crucial, mais s'interroger sur sa pertinence à répondre, seul, à toutes les situations de partage de données l'est aussi.

**D'une part, le rapport de force est déséquilibré entre l'individu et les entreprises demandant le consentement**, souvent détentrices d'un pouvoir technologique et économique important. Le recours au consentement individuel ne doit pas exclure la possibilité d'interdire ou réguler collectivement certaines pratiques, car considérées comme portant un préjudice certain ou ayant un intérêt trop limité pour l'individu ou la société. Dans l'univers médical, si le consentement est un préalable à l'acte, il n'exclut pas l'encadrement des pratiques via l'interdiction de certains actes et leur contrôle par des autorités compétentes. En matière de droit du travail, le contrat que concluent employeurs et employés ne peut déroger aux règles supérieures du droit du travail ou des conventions collectives, qui protègent l'employé et encadrent les pratiques de l'employeur.

Le RGPD, par son double objectif (encadrer les responsables de traitement, conférer des

[24] *Tellement complexe qu'on en fait des taxonomies ! Voir Solove, A taxonomy of privacy.*
[25] *Nissbaum, H. Privacy in context, https://www.sup.org/books/title/?id=8862*
[26] *Warren, Brandeis, The Right to Privacy, Harvard Law Reviez, 1884.*
[27] *« Privacy as trade-offs arising from protecting [as opposed to] sharing of personal data". Voir Acquisti, Taylor and Wagman, The Economics of Privacy, 2016, Journal of Economic Literature, Vol. 54, No. 2, pp. 442–492.*

droits aux individus), répond lui aussi à cette logique mais, volontairement garant de la libre-circulation des données, ne définit pas explicitement de contraintes pour, par exemple, les types de responsable de traitement, de finalités poursuivies ou encore de données collectées[28]. **Le recours au consentement individuel ne doit pas exclure la possibilité d'interdire ou réguler collectivement certaines pratiques**, car considérées comme portant un préjudice certain ou ayant un intérêt trop limité pour l'individu ou la société.

**D'autre part, le consentement est une notion fortement individuelle :** il trahit une approche individualisée, voire individualiste, qui contractualise le rapport entre une entreprise et chaque citoyen pris isolément, au nom de la liberté de la personne. Outre le déséquilibre dans le rapport de forces entre un individu seul et les entreprises, ce caractère individuel du consentement **exclut de fait la dimension collective des données.** Or cette dimension collective est avérée, et l'occulter peut porter préjudice aux individus comme à la société : la valeur des données personnelles est décuplée par leur mise en réseau, les décisions prises par un individu ont un impact sur les données des autres individus[29] et ont des externalités sur l'ensemble des individus.

## PASSER DE L'INDIVIDUEL AU COLLECTIF

Il nous paraît donc urgent, afin de mieux maîtriser la collecte, le partage et les usages des données, de considérer les enjeux de données personnelles comme un problème politique et collectif, qui ne se limite pas au consentement individuel.

Pour davantage prendre en compte la dimension collective des données personnelles, nous n'abandonnons pas le RGPD. Nous proposons plutôt de changer l'approche que nous en avons. Le consentement individuel ex ante et les droits individuels ex post peuvent être enrichis de formes nouvelles d'action collective et de choix collectifs.

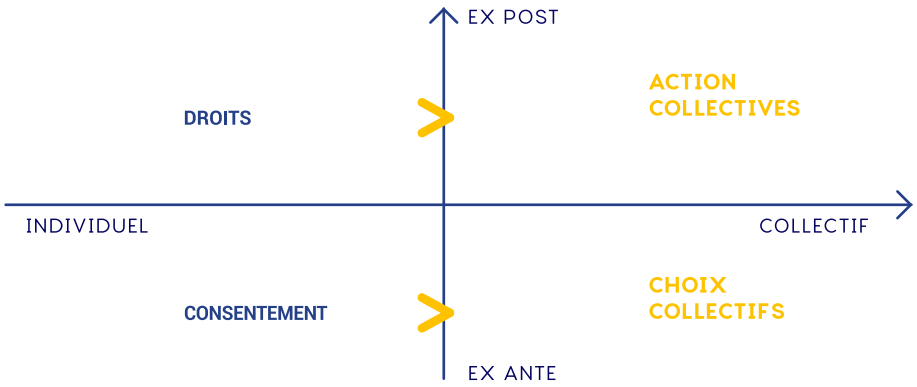


*Figure 8 : Compléter le consentement et les droits individuels par l'action collective et les choix collectifs.*

### CRÉER LES CONDITIONS DE L'ACTION COLLECTIVE EX POST

Le consentement individuel ex ante et la confiance qu'il implique dans le responsable de traitement ne peuvent exclure le contrôle. Celui-ci s'opère aujourd'hui par le régulateur, et nous avons déjà esquissé quelques pistes pour le renforcer. Mais au-delà de la seule action du régulateur, nous pensons que l'action de contrôle pourrait être renforcée quantitativement et qualitativement en créant les conditions de l'inspection par la société civile. Cela passe notamment par l'amélioration de l'exercice des droits individuels, comme évoqué plus haut, mais pourrait être complété par l'obligation de permettre l'exportation facile d'un fil de

[28] *A l'exception, dans son article 9, de données personnelles « qui révèle[nt] l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. »*

[29] *Pour une définition économique : Acemoglu et al., en ligne.*

recommandation individuel ou d'un résultat de recherche. Cela pourrait permettre à terme de créer les conditions de régulation des algorithmes par la foule, par des associations de la société civile ou du monde de la recherche. Une expérience de ce type est mise en œuvre par le Media The Markup, qui met en lumière des biais en rapprochant les recommandations faites par Facebook à différents utilisateurs avec leur origine ethnique ou leurs opinions politiques.

**L'action de la société civile pourrait aussi être facilitée en renforçant les dispositions de l'action de groupe**[30], qui pourrait être rendue plus facilement accessible. A l'heure actuelle, seules trois associations ont le droit d'ester en justice sur des questions de données personnelles, entraînant un problème de bande passante des actions qu'elles sont susceptibles de mener.

## FAIRE DES CHOIX COLLECTIFS EX ANTE

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, et a fortiori dans celle des données personnelles.

**Il nous semble nécessaire d'accroître la participation de la société civile,** par exemple dans des institutions telles que le Conseil National du Numérique et la CNIL. Cela pourrait également être envisagé dans les plateformes structurantes par le biais de comités de parties prenantes; dans le sillage du DMA et du DSA, qui reconnaissent l'influence systémique de ces acteurs, sur le marché ainsi que sur des enjeux démocratiques, on pourrait envisager d'associer plus fortement les citoyens à leur gouvernance, pour les rapprocher de “biens communs”. Les citoyens pourraient par exemple être davantage associés aux évolutions en matière de CGU, aux décisions techniques mais aussi à la définition de lignes directrices pour la collecte, le traitement et l'usage des données personnelles.

**Un problème politique et collectif doit avant tout passer par un débat démocratique.** Ce débat a eu lieu avec la consultation en amont de la Loi pour une République Numérique[31] ou l'entrée en vigueur du RGPD et ses retombées médiatiques, et il gagnerait à être étendu. Cela peut se faire via des commissions parlementaires ad hoc, mais aussi, dans la lignée des expérimentations en matière d'environnement, via une consultation citoyenne sur le numérique, voire par un référendum. 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 les l'accès à l'information.

[30] *Action qui devrait être facilitée par le récent arrêt du 28 avril de la CJUE, ainsi que par la directive européenne sur les recours collectifs.*
[31] *https://www.data.gouv.fr/fr/datasets/consultation-sur-le-projet-de-loi-republique-numerique/*

" LES EXTERNALITÉS DE LA PUBLICITÉ CIBLÉE, DOIVENT-ELLES ÊTRE LAISSÉES AU SEUL CONSENTEMENT DES INTERNAUTES OU FAIRE L'OBJET DE VÉRITABLES CHOIX COLLECTIFS ? "

# V. EXEMPLES : QUELS OBJETS POUR LES CHOIX COLLECTIFS ?

Nous examinons dans cette partie deux applications qui peuvent servir d'exemples concrets pour illustrer les choix collectifs.

Le cadre des données d'intérêt général donne un exemple d'articulation entre le consentement individuel, action collective et choix collectifs concernant le partage de données. Cette articulation n'est pas opérante pour le partage de données dans le secteur de la publicité ciblée, qui repose largement sur le consentement individuel, et cela a des conséquences très concrètes sur les éditeurs de presse.

## EXEMPLE 1 : LES DONNÉES D'INTÉRÊT GÉNÉRAL

La crise sanitaire a relancé le débat sur l'utilisation de données de sociétés privées par la puissance publique et pour l'intérêt général. Nombreux sont ceux qui ont regretté que nous n'ayons pas pu, à l'instar de la Corée du Sud, suivre avec précision les mouvements des personnes infectées pour vérifier leur bon respect de l'isolement et ainsi contrôler plus rapidement l'épidémie de COVID-19. De nombreuses raisons expliquent la différence dans les solutions mises en œuvre, mais nous nous intéressons ici au cadre qui permet **l'utilisation de données privées par la puissance publique.**

**Les données d'intérêt général** ont été introduites en France par la loi pour une République Numérique[32], sans avoir une réelle portée normative en dehors des entreprises délégataires d'un service public. La loi prévoit néanmoins l'utilisation au cas par cas et dans une approche sectorielle de certaines données issues du secteur privée par la puissance publique : données de mobilité, données de logement…

Le rapport issu de la mission confiée au député Eric Bothorel[33] réaffirme le besoin de définir plus clairement ces données d'intérêt général, notamment dans des cas où la puissance publique n'est pas à même de produire des données avec la même qualité que le secteur privé, et d'esquisser une doctrine pour ces données d'intérêt général. Il souligne l'intérêt que peuvent présenter pour le suivi des restrictions sanitaires les traces numériques ou les données de transaction bancaires, comme ce fut le cas en Corée, et rappelle que certaines entreprises conduisent déjà des partenariats en partageant des données agrégées pour la recherche, la régulation ou l'élaboration de politiques publiques.

**En principe, l'exécution d'une mission d'intérêt public est une des six bases légales de traitement[34] prévues par le RGPD**. Une entreprise privée n'est donc pas tenue d'obtenir le consentement de l'utilisateur pour partager des données d'intérêt général avec la puissance publique.

**Néanmoins, le rapport Bothorel préconise d'avoir recours au consentement** « dans une logique d'autodétermination informationnelle », facteur d'acceptabilité sociale du partage de données d'intérêt général. Le Data Governance Act introduit même la notion d'**« altruisme des données »**, qui permettra à des individus (mais aussi des entreprises) de donner leur consentement pour le partage de leurs données personnelles. Ce partage peut se faire directement avec la puissance publique, mais peut aussi être intermédié par un tiers de confiance. Cette solution, dont le *Digital Governance Act* comme le rapport Bothorel pensent

[32] *https://www.economie.gouv.fr/republique-numerique-ouverture-donnees-d-interet-general*
[33] *Bothorel E., Pour une politique publique de la donnée, 2020. Les conclusions sont notamment nourries d'une consultation sur des cas d'usages acceptables de données d'intérêt général.*
[34] *dans l'article 6 du RGPD,*

qu'elle permet de pallier la défiance envers l'Etat, peut aller plus loin et devenir le fondement de « communs de la donnée ».

Selon nous, **le recours au consentement dans le cadre des données d'intérêt général est une bonne chose**, alors même qu'un rapport sénatorial préconise la collecte de données sanitaires en temps de crise[35] sans mention du consentement. Cependant, les mêmes questions se posent que dans le cas du partage de données entre entreprises privées : le consentement n'en sera pas moins dévoyé. Il nous semble nécessaire de s'assurer de l'existence d'un consentement libre et éclairé, mais aussi d'alternatives claires.

Le consentement individuel seul ne peut suffire. La confiance et la bonne information du citoyen passent par la possibilité à celui-ci d'agir ex post sur ces données et ex ante dans la co-construction des solutions. Elle passe aussi par l'existence d'un débat sain et un portage politique fort.

Ces précautions sont pour nous la seule manière de prévenir les abus, garantir la confiance des citoyens, une sécurité juridique et réputationnelle à tous les acteurs et de rendre possible certaines applications innovantes dans l'exploitation des données privées par la puissance publique.

## EXEMPLE 2 : LA PUBLICITÉ CIBLÉE

La publicité ciblée est l'un des plus forts moteurs de collecte, de traitement et d'usages des données. Il convient donc de s'interroger sur ses impacts et son utilité. Aujourd'hui, le partage de données pour la publicité ciblée est aux mains de l'internaute via le consentement. Comme nous l'avons montré, cette demande de consentement est rarement libre et éclairée, et s'inscrit dans un rapport de force déséquilibré. Pour l'internaute, se voir proposer un produit plutôt qu'un autre (et donc des publicités plus pertinentes) peut réduire ses coûts de recherche et le nombre de publicités qu'il voit, mais ces avantages doivent être considérés au regard du caractère intrusif de certaines publicités.

Pour les autres acteurs économiques, l'utilité pose aussi question. En effet, si l'efficience des publicités ciblées est mise en avant, leur prix sur le marché est aujourd'hui jusqu'à 4 à 5 fois supérieur aux publicités contextuelles. Cette valeur est partagée entre les (très) nombreux acteurs de la chaîne programmatique[36], mais sa répartition pose question. Ainsi, le secteur est dominé par un duopole Google et Facebook : ces deux entreprises contrôlent à elles seules 75% du marché français. L'amende record de l'Autorité de la Concurrence à Google montre aussi l'existence d'abus de position dominante[37].

Au total, l'AdTech capte l'essentiel de la valeur au détriment des éditeurs de contenu, qui « voient leur ressource publicitaire se tarir, leur relation de dépendance aux plateformes se renforcer et leur modèles économiques se fragiliser. »[38]

Le *rapport Publicité en ligne : pour un marché à armes égales,* propose diverses solutions pour améliorer le partage de valeur entre acteurs : aligner le cadre juridique du display en ligne sur celui de la télévision, activer la *brand safety* pour suivre les publicités, soutenir la création d'identifiants uniques, mais surtout, il propose d'agir sur le pouvoir de marché (avec des propositions qui rejoignent en de nombreux points le projet de *Digital Markets Act*).

Si cet aspect concurrentiel est essentiel, il ne peut pas occulter la question des données personnelles. Le partage de ces données est un élément fondateur de la publicité en ligne, et les enjeux de protection de la vie privée doivent être pris en compte dans l'organisation

[35] *Ces sénateurs proposent la création d'un Crisis Data Hub, à lire en ligne.*
[36] *Le secteur de la publicité en ligne a généré 5,1 Md€ de revenus en 2019 en France, en hausse de 13 % sur un an. Voir Perrot, A., Emmerich, M., Publicité en ligne : pour un marché à armes égales, 2020, IGF.*
[37] *https://www.lemonde.fr/pixels/article/2021/06/07/publicite-en-ligne-l-autorite-de-la-concurrence-inflig e-a-google-une-amende-de-220-millions-d-euros_6083210_4408996.html*
[38] *Ibid.*

d'un marché de la publicité en ligne plus souhaitable. Nous avons essayé de formuler des solutions « pragmatiques » : encadrement du régime des co-traitants pour la publicité ciblée, renforcement de l'application du droit d'accès.

La question de l'interdiction, ou a minima, de la régulation de la publicité ciblée, se pose[39] : le jeu en vaut-il la chandelle ? Les externalités de la publicité ciblée, parmi lesquelles le partage de données personnelles et ses conséquences, doivent-elles être laissées au seul consentement des internautes ou faire l'objet de véritables choix collectifs, précisant les conditions, et acceptant le cas échéant les conséquences ?

## DES ÉDITEURS DE PRESSE SANS PUBLICITÉ CIBLÉE ?

Ces questionnements au sujet de la publicité ciblée ne peuvent être examinés à l'aune de leurs conséquences sur un domaine en particulier : les éditeurs de contenu en ligne et les sites de presse. En effet, aujourd'hui, de nombreux titres de presse se financent en grande partie par la publicité ciblée : en moyenne, 60% des recettes de la presse seraient issues du digital, et parmi celles-ci, entre 40 et 50% seraient issues de la publicité (le reste provenant des abonnements)[40]. Faire un choix sur la publicité ciblée a donc des conséquences immédiates sur le mode de financement des éditeurs de contenu en ligne.

Les éditeurs de presse sont aujourd'hui les plus fervents défenseurs de la collecte de données. Ils ne sont pas non plus les meilleurs élèves : on trouve un nombre très élevé de cotraitants sur leurs sites, certains mettent en place les fameux *cookie walls*, ou trouvent des outils pour sécuriser la collecte de données. Par exemple, en réaction aux nouvelles lignes directrices de la CNIL et à la suppression des cookies tiers (voir annexe 3 du rapport), six d'entre eux ont lancé un identifiant commun, le « Pass media »[41] afin de poursuivre la collecte de données pour la publicité dans un environnement logué, sans dépendre des cookies tiers ou de trop nombreuses bannières de consentement.

La dépendance à la publicité ciblée est aussi, on l'a montré, une dépendance aux GAFAM et au monde de l'*AdTech,* qui captent une grande partie des revenus publicitaires. Afin de réduire cette dépendance, de nombreux titres défendent des modèles par abonnements, avec ou sans *cookie wall*. S'il est une garantie de revenus, ce modèle suppose un lectorat déjà acquis, qui fonctionne pour les grands médias (Le Monde, Les Echos) ou les médias indépendants (Mediapart), et n'exclut pas un partage de données large.

La généralisation des modèles d'abonnements aboutit néanmoins à un autre problème : celui de l'accès à l'information. La prédominance d'un modèle par abonnement où avec des *cookies walls* pourrait renchérir l'accès à une information de qualité, et de ce fait poser un problème démocratique majeur. Cela supposerait également un revirement fort du mode de consommation actuel de l'information par les jeunes générations, qui sont plus susceptibles d'aller picorer l'information auprès de divers médias, parfois par l'entremise d'un réseau social. La diminution du nombre de sources accessibles pour chaque lecteur renforcerait les risques de bulles informationnelles, enjeu majeur à l'heure ou la lutte contre les fake news occupe une place grandissante dans les politiques publiques.

Parmi les pistes envisagées actuellement pour financer la presse, aucune ne semble pleinement convaincante. Les agrégateurs de contenus peinent à émerger sauf sur des marchés de niche comme les étudiants, faute d'accord entre les acteurs et faute de l'existence d'un marché. Les réformes des droits voisins actuellement menées, qui visent à rediriger une partie de la valeur captée par les GAFAM vers les médias en ligne, les rendrait encore plus

[39] *Lau Y., A Brief Primer on the Economics of Targeted Advertising, FTC Issue Paper, 2020, en ligne.*
[40] *Chiffres provenant d'un entretien avec un acteur de l'AdTech.*
[41] *Initiative sous la tutelle du Geste, une association d'éditeurs, à lire en ligne.*

dépendants financièrement de ces plateformes.

Dès lors, un remplacement de la publicité ciblée individualisée par la publicité contextuelle entraînerait une chute des revenus provenant de la publicité en ligne qui devra être accompagnée par l'Etat, à travers différents dispositifs de soutien, directs ou à l'émergence de solutions comme les agrégateurs. Il s'agit d'un enjeu démocratique majeur : l'indépendance de la presse nationale dans ses sources de financement, notamment vis-à-vis de grands acteurs étrangers, est un enjeu de souveraineté pour les médias français et européens, et un gage de qualité du débat démocratique.[42]

[42] *https://www.lopinion.fr/edition/international/guillaume-klossa-il-ne-peut-y-avoir-souverainete-politique -178529*

# CONCLUSION

Nos propositions visent à créer les conditions pour que le partage de données par le citoyen s'effectue en confiance, en accentuant sa liberté de choix, la transparence des usages qui en sont faits, et en permettant au débat démocratique de s'en emparer. Comme la protection de l'environnement, la protection des données personnelles est un problème collectif et doit être traité comme tel.

Nous ne voulons surtout pas sonner le glas de la mise en commun de données personnelles. Celle-ci présente de très nombreuses applications souhaitables par la société, dans des domaines comme la santé, l'administration publique, ou la création de nouveaux services L'objet de nos propositions n'est pas de générer des frictions rendant impossible tout partage de données, mais bien de créer les conditions pour que les partages soient acceptables par les citoyens, ce qui est nécessaire pour la poursuite de l'innovation liée au partage de données personnelles sur le long terme.

La bonne nouvelle, c'est que les outils existent. En poursuivant la discussion autour du RGPD, en améliorant sa mise en œuvre, mais aussi en osant questionner certaines pratiques, nous pouvons rendre la collecte, le traitement et le partage de données plus responsable.

# NOS PROPOSITIONS

## 1. AMÉLIORER L'EFFECTIVITÉ DES DROITS

en encadrant le recours aux co-traitants pour la publicité en ligne, en renforçant et facilitant l'exercice du droit d'accès et en renforçant la coopération entre régulateurs européens.

## 2. RENDRE LE CONSENTEMENT VÉRITABLEMENT LIBRE ET ÉCLAIRÉ

en sensibilisant les utilisateurs, en améliorant l'expérience utilisateur, en régulant davantage le design et interdisant le cookie wall, et en donnant véritablement le choix à l'utilisateur.

## 3. MIEUX ARTICULER LE CONSENTEMENT ET LES DROITS INDIVIDUELS AVEC LES CHOIX POLITIQUES ET LES ACTIONS COLLECTIVES :

en renforçant les dispositions de l'action de groupe, en redonnant sa place à la société civile dans la régulation et les entreprises du numérique.

Digital New Deal

# NOS REMERCIEMENTS

Ce papier est le fruit de plusieurs mois d'enquête dans le cadre de notre mémoire d'ingénieurs des mines. Il s'appuie aussi sur le rapport commun réalisé avec les élèves de l'école nationale d'administration. Nous les remercions chaleureusement pour la qualité des échanges sans lesquels ce travail n'aurait pas pu voir le jour : Adrien, Quentin, Paul, Marie, Nicolas, Alexandre, Maximilien, Jenny, Camille, Arnaud, Aurélien, Shinya, Lena et Marie.

Nous tenons à remercier toutes les personnes qui ont contribué et avec lesquelles nous nous sommes entretenus.

Nous remercions tout particulièrement Pierre Fleckinger, professeur d'économie à l'école des Mines, pour son important apport et son soutien sans faille durant toutes les étapes de ce travail.

Pour finir, nous remercions le think-tank, et tout particulièrement Axelle Lemaire et Arno Pons, pour leur accompagnement dans la publication de cette note.

# DIGITAL NEW DEAL
# LE THINK-TANK DE LA NOUVELLE DONNE

Digital New Deal accompagne les décideurs privés et publics dans la création d'un Internet des Lumières, Européen et Humaniste. Notre conviction est que nous pouvons offrir une 3eme voie numérique en visant un double objectif : défendre nos valeurs en proposant une nouvelle régulation contre la centralisation des pouvoirs ; et défendre nos intérêts en créant les conditions de la coopération face à la captation de la valeur par les « Big Tech ».

Notre activité de publication a pour vocation d'éclairer de manière la plus complète possible les évolutions à l'œuvre au sein de enjeux de « souveraineté numérique », dans l'acception la plus large du terme, et d'élaborer des pistes d'actions concrètes, voire opérantes via le Do tank, à destination des organisations économiques et politiques.

## LE CONSEIL D'ADMINISTRATION

Olivier Sichel (président fondateur) et Arno Pons (délégué général), pilotent les orientations stratégiques du think-tank sous le contrôle régulier du conseil d'administration.

Forts de leur intérêt commun pour les questions numériques, les membres du Conseil d'administration ont décidé d'approfondir leurs débats en formalisant un cadre de production et de publication au sein duquel la complémentarité de leurs expériences pourra être mise au service du débat public et politique. Ils s'impliquent personnellement dans la vie de Digital New Deal, notamment dans le choix des rapports et de leurs rédacteurs. Il sont les garants de notre indépendance, académique et économique.

SÉBASTIEN BAZIN
PDG AccorHotels

NATHALIE COLLIN
DG branche Grand Public et Numérique Groupe La Poste

NICOLAS DUFOURCQ
DG de Bpifrance

AXELLE LEMAIRE
Ex-Secrétaire d'Etat du Numérique et de l'Innovation

ALAIN MINC
Président AM Conseil

DENIS OLIVENNES
DG Libération

YVES POILANE
DG Ionis Education Group

ARNO PONS
Délégué général du think tank Digital New Deal

JUDITH ROCHFELD
Professeur agrégée de Droit, Panthéon Sorbonne

OLIVIER SICHEL
President Digital New Deal
DGA Caisse des Dépôts

BRUNO SPORTISSE
PDG Inria

ROBERT ZARADER
PDG Bona fidé

# NOS PUBLICATIONS

Fiscalité numérique, le match retour | Vincent Renoux - *septembre 2021*

Défendre l'état de droit à l'ère des plateformes | Denis Olivennes et Gilles Le Chatelier - *juin 2021*

Cloud de confiance : un enjeu d'autonomie stratégique pour l'Europe | Laurence Houdeville et Arno Pons - *mai 2021*

Livres blancs : Partage des données & tourisme | Fabernovel et Digital New Deal - *avril 2021*

Partage de données personnelles : changer la donne par la gouvernance | Matthias de Bièvre et Olivier Dion - *septembre 2020*

Réflexions dans la perspective du Digital Services Act européen | Liza Bellulo - *mars 2020*

Préserver notre souveraineté éducative : soutenir l'EdTech française | Marie-Christine Levet - *novembre 2019*

Briser le monopole des Big Tech : réguler pour libérer la multitude | Sébastien Soriano - *septembre 2019*

Sortir du syndrome de Stockholm numérique | Jean-Romain Lhomme - *octobre 2018*

Le Service Public Citoyen | Paul Duan - *juin 2018*

L'âge du web décentralisé | Clément Jeanneau - *avril 2018*

Fiscalité réelle pour un monde virtuel | Vincent Renoux - *septembre 2017*

Réguler le « numérique » | Joëlle Toledano - *mai 2017*

Appel aux candidats à l'élection présidentielle pour un #PacteNumérique | *janvier 2017*

La santé face au tsunami des NBIC et aux plateformistes | Laurent Alexandre - *juin 2016*

Quelle politique en matière de données personnelles ? | Judith Rochfeld - *septembre 2015*

Etat des lieux du numérique en Europe | Olivier Sichel - *juillet 2015*

**contact@thedigitalnewdeal.org**

**www.thedigitalnewdeal.org**


*mai 2022*

www.thedigitalnewdeal.org