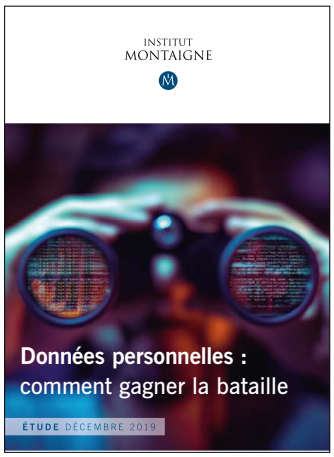


# Résumé

« **Les gentlemen ne lisent pas le courrier des autres ».** En réalité, ils le font parfois, légalement ou subrepticement. Nous émettons constamment des données à caractère personnel et celles-ci flottent dans le cyberespace. **L'ère numérique ne peut être désinventée, et il ne peut y avoir de droits individuels sans respect de la vie privée.** La manière dont les sociétés relèvent ce défi est donc une question qui nous concerne tous.

Sur les enjeux de respect de la vie privée numérique et de protection des données personnelles, l'Institut Montaigne offre un éclairage des principaux **cadres réglementaires – Union européenne, Inde, Chine et États-Unis en toile de fond.** À partir de cette comparaison, nous identifions des améliorations souhaitables pour le Règlement Général sur la Protection des Données (RGPD).

Le respect de la vie privée est intuitivement compris de tous, mais plus difficilement défini. **Légalement, il s'exprime par la protection des données,** et les données à caractère personnel sont le point central de ces règles.

**L'objectif de protéger les données à caractère personnel** et de **garantir la vie privée** est en balance, sur le plan réglementaire, avec deux autres buts : **l'efficacité économique** et **l'intérêt public** (de la sécurité nationale à tout ce qui peut s'apparenter à un bien public). Toutes les régulations naviguent entre ces trois objectifs.

**Le débat sur le respect de la vie privée a deux matrices.** L'une se trouve aux **États-Unis.** Les technologies numériques y ont été largement inventées, tandis que les entreprises, grandes ou non, pionnières dans ces technologies ont une **influence mondiale.** L'Amérique est dès lors la mère de tous les débats sur la vie privée, et elle a précédemment promulgué d'importantes mesures législatives, fédérales ou locales.

**L'Union européenne** est devenue l'autre acteur influent avec **son RGPD**. Cependant, ce dernier est un **texte très général à certains aspects,** construit sur un équilibre fragile entre des objectifs contraires.

## Le RGPD, une prouesse réglementaire européenne

Avec ses **88 pages superbement écrites,** se concentrant sur la collecte et le traitement des données à caractère personnel, le RGPD crée un équilibre entre **protection des personnes physiques, nécessité commerciale** de libre circulation des données, et exemptions de cette protection lorsque des exigences légales ou l'**intérêt public** sont en jeu.

L'une des innovations du RGPD est de prévoir une coopération entre autorités nationales pour les **affaires transfrontalières.** Celle-ci passe par un mécanisme de **guichet unique**, où une autorité de contrôle « chef de file » doit d'abord être désignée. Cependant, la réalité est moins impressionnante car le mécanisme ne s'applique pas si l'entité qui est en cause exerce ses activités en dehors de l'UE. De la même manière, ce mécanisme ne différencie pas assez précisément l'établissement légal du lieu d'exercice réel des opérations de cette entité. Dès lors, le risque est évidemment celui de **28 guichets différents.**

Les amendes infligées sont basées sur des montants ***ex ante,*** avec des plafonds proportionnels au chiffre d'affaires. Les sanctions devraient aussi s'appuyer sur des **actions en dommages *ex post,*** et ceci implique très largement une bascule vers une **réelle évaluation des dommages causés** et donc des recours en justice. La raison est simple : les **entreprises font souvent un calcul coûts/bénéfices** pour se conformer au règlement. Les individus devraient obtenir des réparations, y compris par des actions de groupe, en cas de violation de leur vie privée.

**La technologie est une frontière qui évolue rapidement,** et il est impossible de prédire quels types de données deviendront personnelles, sensibles ou critiques. Les données collectées ne peuvent souvent être complètement effacées. Ce qui peut être plus sûrement réglementé, c'est l'**usage qui est fait des données collectées,** y compris dans leur interprétation.

Notre tableau de la protection des données inclut deux études de cas sur l'**Inde** et la **Chine**. L'Inde est le plus grand marché mondial de données et a le plus grand nombre d'usagers au monde. La Chine occupe une place de plus en plus stratégique dans les débats concernant le respect de la vie privée.

## L'Inde, un mix numérique entre l'UE et la Chine

Après la décision de la **Cour suprême de l'Inde** sur le respect de la vie privée comme garanti par la constitution, le **projet de loi *Personal Data Protection Bill*** (PDPB) a été rédigé par un groupe d'experts en 2018 et approche le stade de l'examen législatif. Il suit largement le RGPD, fixant des obligations aux fiduciaires de données et accordant des droits aux individus. Il met en place une **autorité nationale de protection des données,** introduit des pénalités financières en cas de non-conformité, mais **autorise largement les pouvoirs publics à outrepasser les restrictions en cas d'atteinte à la sécurité nationale ou à l'intérêt public.**

L'**Inde est aussi une société mouvante,** un terrain de bataille pour les questions de respect de la vie privée, de la souveraineté sur les données ou de leur libre circulation. Avec des inquiétudes sur la sécurité des données des applications chinoises et la prédominance des GAFA américaines dans le commerce en ligne, **certains militent pour une localisation des données au nom de la souveraineté et de la sécurité.** Cette revendication est souvent considérée comme un soutien à l'industrie et aux entreprises locales. L'Inde semble ainsi être un **pont** entre le modèle européen et celui de la Chine. Elle s'inspire **du RGPD pour définir sa législation mais utilise la souveraineté comme un outil de politique industrielle.**

Le PDPB laisse **à la discrétion du gouvernement central** des décisions importantes. Le contrôle sur l'espace numérique se

retrouve dans des instruments tels que des lignes directrices sur la modération de contenu pour des intermédiaires de données. L'accès facilité aux données et codes sources se retrouve dans le projet de loi sur les intermédiaires de données et celui sur le commerce en ligne. Ainsi, **la régulation peut aussi pencher vers le modèle chinois, mettant en exergue la sécurité nationale et le contrôle de la libre circulation des données.**

## La Chine, l'État-surveillance avec les inquiétudes qui en découlent sur la protection de la vie privée

Avec la **Chine**, nous entrons dans un tout autre monde. Derrière son pare-feu, ceux que l'on appelle les « BAT » (Baidu, Alibaba et Tencent) **collectent et traitent plus de *big data* que n'importe quel autre concurrent étranger.** En pratique et même avec une réglementation assez lacunaire sur ce point, le gouvernement a un accès illimité aux données. Le débat public général sur le respect de la vie privée est dès lors axé sur la **sécurité des données** dans le cadre de la **sécurité nationale,** plutôt que sur la protection de la vie privée.

La loi sur la cybersécurité de la Chine (2017) offre en principe une protection aux usagers. Toutefois, elle est biaisée en faveur des **droits de l'État,** ceux des **individus** étant **vagues ou conditionnels.** Cette loi fondatrice a été suivie d'une série d'autres lois, réglementations et normes supplémentaires. La plus importante est la **spécification *Personal Information Security*** (PIS) de 2018, qui emprunte certaines caractéristiques au RGPD mais diffère sur d'autres. **Son obligation de consentement est moins stricte**, le résultat d'un compromis trouvé entre représentants des entreprises et des experts.

L'État de surveillance chinois peut concevoir de protéger les individus en tant que consommateurs contre les intérêts commerciaux prédateurs. Il ne l'accepte pas contre lui-même. Les lois et réglementations peuvent être **interprétées à volonté,** au moyen de **catégories « autres » mal définies.**

## Données de santé et respect de la vie privée : un tournant positif

Le secteur de la santé est notre étude de cas. La **santé numérique** a initié une révolution en accélérant la **recherche** et en facilitant les soins au contact des patients. Mais tout ceci repose sur une **connaissance et une prédictibilité extrêmement fortes de l'état de santé d'un individu.** Dès lors, pour la protection de la vie privée, cela introduit des défis essentiels, les plus importants qu'on puisse trouver en dehors du cas d'un État de surveillance.

Dans ce domaine, le RGPD n'a que des prescriptions génériques, en restant plus ouvert à **l'utilisation de données médicales par des entités publiques que par des assureurs ou des entreprises de santé privés.** Les Européens ont depuis longtemps construit des bases de données de santé analogiques ou numériques pour leurs Etats-providence. Mais celles-ci étaient **régulièrement collectées pour des remboursements** plutôt que pour des raisons médicales, ou *a fortiori* pour la recherche. La **France** par exemple, malgré une impulsion désormais ferme en termes de politique publique, n'est qu'à mi-chemin sur ces questions.

L'approche **indienne** paraît pour l'instant sommaire sur le front réglementaire, alors que des évolutions numériques majeures sont en cours. Une importante loi sur la protection des données personnelles de santé, **DISHA,** a été soumise au Parlement. Elle est si protective des données qu'elle sera difficile à appliquer, ou sera un **frein à la recherche médicale.**

En revanche, les stratégies numériques **chinoises** conçoivent les données de santé comme partie intégrante du développement médical et de l'industrie pharmaceutique en tant que **ressource économique.** Il y a peu de garde-fous, et la Chine encourage les entreprises étrangères à utiliser son **cadre réglementaire laxiste** sur le *big data.*

## Proposition 1 : Renforcer le contrôle, l'application et l'adaptabilité du RGPD

Une règle n'est jamais meilleure que sa mise en œuvre réelle. Un RGPD révisé devrait éviter les restrictions nuisant à un processus de décision unique. Il devrait mettre l'accent sur la clarté, la simplicité et la facilité de la mise en œuvre

## Proposition 2 : Rendre les politiques de confidentialité plus lisibles et ergonomiques

L'expérience utilisateur (UX) est aussi importante que la compréhension des règles par les utilisateurs. L'amélioration de l'expérience utilisateur est essentielle pour atteindre l'un des objectifs premiers du RGPD : permettre aux particuliers de reprendre le contrôle de leurs données personnelles.

## Proposition 3 : Assurer le respect effectif de la vie privée dès la conception *(privacy by design)*

Les individus devraient être déchargés de décisions qu'ils ne peuvent prendre, et il y a dès lors un besoin de politiques, de lignes directrices et d'instructions claires en matière de respect de la vie privée dès la conception.

## Proposition 4 : Donner le droit effectif d'obtenir une explication dans le cadre du RGPD

Le public a le droit d'obtenir une explication quant aux décisions prises par un traitement automatisé. L'explicabilité, la fiabilité, la responsabilité et la transparence des algorithmes doivent être garanties, particulièrement dans le secteur public.

## Proposition 5 : Créer la possibilité de recours en responsabilité et dommages *(tort and litigation)*

Réguler requiert aussi de s'appuyer sur des actions *ex post,* et de créer un cadre imposant une plus grande responsabilité délictuelle. En échange de la mise en place de recours judiciaires en responsabilité *ex post,* l'exigence de transparence des algorithmes privés pourrait être moindre.

## Proposition 6 : Introduire des réglementations sectorielles

Certains secteurs ont besoin d'une réglementation spécifique et plus précise. Celle-ci devrait être encouragée dans le secteur de la santé, des services financiers et des données de la police.

## Proposition 7 : Créer des données de santé simulées pour améliorer l'anonymisation

Les données de santé simulées sont une technologie nouvelle qui apporte des solutions tant pour les besoins de la recherche sur le *big data* en matière de santé que pour les garanties de confidentialité des données. Des études complémentaires sont nécessaires sur l'équilibre à tenir concernant ces deux nécessités.