



Entraîner une IA sans posséder la donnée est possible

10 sept. 2019 • 9 min read

L'intelligence artificielle, véritable révolution du XXI^e siècle, a un large spectre d'applications possibles mais se heurte dans bien des cas à la problématique de l'accès aux données : comment obtenir une base de données suffisamment riche pour avoir des résultats précis ? Comment accéder à des données potentiellement privées en respectant une certaine éthique ? Comment utiliser ces techniques dans des contextes où les informations atteignent des niveaux extrêmes de sensibilité (sociologie, recherche médicale, ...) ?

Rendue possible par des infrastructures toujours plus puissantes en calculs, l'intelligence artificielle (IA) ouvre de nombreuses portes dans la santé, l'industrie, l'énergie ou dans la vie de tous les jours. Derrière cette appellation se cachent plusieurs théories mathématiques : *régression, réseau de neurones, machine à vecteurs de support, méthode des k plus proches voisins*, etc. Ces différentes manières de concevoir l'intelligence artificielle ont en commun la capacité de synthétiser de l'information pour rendre compte d'un phénomène. La modélisation construite peut être utilisée pour prédire une information (avec une certaine marge d'erreur), étudier des interactions, ou encore essayer de simuler le réel.

FaceApp merely highlights how much we've already lost control of our digital data. (*FaceApp ne fait que souligner à quel point nous avons déjà perdu le contrôle de nos données numériques.*) ([MIT Technology Review](#))

Grâce à l'intelligence artificielle, il était déjà possible de lire automatiquement vos chèques, ou reconnaître les éléments présents sur une photo, vous permettant ensuite de la chercher par mots clés. Il est maintenant possible de créer une vidéo de toute pièce, donnant naissance aux [DeepFakes](#). C'est dans ce contexte que s'est popularisée l'application mobile FaceApp, qui utilise une photo de votre visage pour vous vieillir, vous rajeunir, vous faire sourire et qui par la même occasion collecte vos données personnelles ([En savoir plus : Applications de retouche photo : les conseils de la CNIL](#)).



Cet article présente comment, chez [Cozy Cloud](#), nous concevons l'intelligence artificielle. L'IA doit être responsable de l'utilisation qui est faite de vos données, dès lors que vous avez accepté de les partager. C'est pourquoi, nous avons conçu un protocole où la donnée n'est pas associable à votre identité et n'est jamais conservée en dehors de votre espace personnel.

L'intelligence artificielle et son besoin de ressources

Pour entraîner une intelligence artificielle, il faut de la donnée. Beaucoup de données. D'où l'importance de disposer d'une grande puissance de calcul.

Cependant, la donnée d'apprentissage est parfois difficile d'accès.

Comment former une base de données suffisamment riche en diversité et importante en volume pour concevoir une intelligence artificielle performante ?

Dans certains contextes, les [scientifiques de la donnée ou Data Scientist en anglais](#) peuvent se reposer sur l'Open Data : car de plus en plus de compagnies ou d'acteurs publics accordent un libre accès à des bases de données, à l'instar du [service de transports de l'agglomération rennaise](#). Le problème de cette solution est qu'elle est restreinte à des données ayant généralement peu de valeur marchande, parce que relativement facile à produire et par nature, souvent publique. Comme toute matière première, plus la donnée est rare ou confidentielle, plus elle est difficile à obtenir. C'est pourquoi [elle se revend à prix d'or](#) et s'acquiert de manière discrète.

Ainsi, il faut trouver un autre moyen de collecter des données. Une autre solution serait d'avoir recours à des "[data brokers](#)". Mais les scandales à répétition et la manière dont les données sont collectées suffisent à mener au rejet de cette hypothétique solution.

Il est anormal de se servir directement dans les album photos ou l'historique de localisation de ses utilisateurs pour collecter la moindre information et utiliser des méthodes statistiques pour en deviner d'autres. C'est pourquoi la réglementation impose que les utilisateurs acceptent de livrer une partie de leurs données via l'acceptation des conditions générales. Cependant, il serait préférable que l'utilisateur accepte, non pas pour enlever une [agaçante pop-up](#), mais parce qu'il a réellement confiance dans l'utilisation respectueuse qui sera faite de ses données personnelles.

Dans certains contextes, il est possible d'ajouter un filtre pour anonymiser puis un second pour empêcher la ré-identification des utilisateurs. C'est, par exemple, le cas des données présentant un certain niveau d'agrégation (e.g. le salaire moyen par commune), sur lesquelles, il est possible d'appliquer des techniques de *confidentialité différentielle*. Cela suppose de modifier les données utilisateur (e.g. le salaire) au cas par cas en influant que faiblement sur le résultat final (e.g. notre salaire moyen). Cette même technique est utilisée par Apple ou par Google, notamment dans le module d'intelligence artificielle [TensorFlow Privacy](#).

La confidentialité différentielle est efficace dans certain cas, mais ne peut pas toujours s'appliquer. Comment protéger la vie privée de ces derniers quand

l'élément intéressant pour l'apprentissage permet de remonter directement à eux (e.g. un visage sur une photographie) ? Il est coûteux, voire impossible d'anonymiser quand l'algorithme a précisément besoin de données permettant de vous identifier pour apprendre convenablement. Aussi, deuxième problème présentée par l'anonymisation et la confidentialité différentielle, comment garantir que nul ne peut associer la donnée à son utilisateur au moment de la transmission ? Ces problématiques sont fondamentales pour bâtir une IA respectueuse de la vie privée et c'est à ces questions que nous proposons une solution.

Contribuez tout en gardant le contrôle sur vos données

Chez [Cozy Cloud](#), nous tenons à ce que vous gardiez les pleins pouvoirs sur vos données personnelles. Si une intelligence artificielle a besoin d'entrer dans votre sphère privée, elle doit le faire d'une manière transparente et succincte.

Nous développons actuellement une solution, respectant la confidentialité dès la conception, pour effectuer des calculs sur un ensemble de domiciles numériques Cozy : **DISPERS**. Ce protocole est issu d'une thèse CIFRE entre Cozy Cloud et [l'équipe PETRUS de l'INRIA Saclay](#). Plus qu'un anonymat, ce protocole apporte des garanties fortes qu'un calcul portant sur des données personnelles ne dévoilera aucune information tout au long de son exécution. Ces travaux ont donné lieu à deux publications académiques :

- *Julien Loudet, Luc Bouganim, Iulian Sandu Popa* [Privacy-Preserving Queries on Highly Distributed Personal Data Management Systems](#)
- *Julien Loudet, Iulian Sandu Popa, Luc Bouganim* [SEP2P: Secure and Efficient P2P Personal Data Processing](#).

Le protocole DISPERS s'intègre également dans [le projet ANR PerSoCloud](#), une coopération entre Cozy Cloud, Orange, INRIA Saclay et l'Université de Versailles Saint-Quentin-en-Yvelines, qui a pour objectif de faciliter la mise en relation du domicile numérique personnel de chacun.

DISPERS propose ainsi une manière de distribuer les tâches et informations entre plusieurs domiciles numériques Cozy qui seront co-réaliseurs du traitement. Le protocole incorpore des procédés pour cacher les détenteurs de l'information ou

rendre les données incompréhensibles par l'acteur qui sera responsable d'une sous-tâche. Ainsi aucun acteur n'est en mesure de compromettre le calcul et, dans une certaine limite, ce qu'il manipule !

Ce protocole étant indépendant des plateformes de Cloud personnel, nous l'avons adapté pour l'intégrer dans l'architecture Cozy et faire en sorte que les calculs soient effectués par un ensemble de serveurs de confiance dont la sécurité et l'intégrité présentent idéalement des garanties par construction.

Des requêtes distribuées respectant la confidentialité

Imaginons un million de domiciles numériques Cozy répartis sur différents hébergeurs (n'importe qui pouvant héberger son Cozy). Imaginons, de plus, qu'ils contiennent tous une même information : le rythme cardiaque moyen de l'utilisateur sur le dernier mois. Information qui aura, par exemple, pu être importée depuis une montre connectée.

Nous aimerais maintenant connaître l'articulation de cette statistique sur plusieurs tranches d'âge. En d'autres termes, nous aimerais connaître le rythme cardiaque moyen des 12-25 ans, des 25-50 ans et des 50-100 ans.

Cette information peut s'exprimer sous la forme d'une requête, qu'il faut comprendre ici comme l'interrogation d'une base de données. Obtenir l'âge moyen d'un groupe d'individus depuis une base de données, c'est effectuer une requête. Nous parlons ici de requêtes distribuées parce que l'information n'est pas centralisée au sein d'une unique base de données. Si l'on reprend notre exemple du rythme cardiaque, l'information est stockée sur un ensemble de bases de données (les domiciles numériques Cozy). Les rythmes cardiaques moyens doivent être collectés avant d'être moyennés.

Pour mettre en place la requête, nous avons besoin de serveurs de calcul propres au protocole. Les communications des serveurs avec l'extérieur sont chiffrées et les traitements idéalement isolés dans un [environnement d'exécution de confiance](#).

Sous-tâches du processus inspiré de DISPERS et flux échangé entre les différents acteurs

Le Querier (Q) est l'utilisateur déclenchant la requête en envoyant certaines informations chiffrées au Conductor. La couleur d'un flux, sur le schéma ci-dessus, correspond à la couleur de l'unique acteur capable de déchiffrer l'information.

Les deux premières étapes d'une requête sont la recherche et l'interrogation des individus. Nous avons tout un ensemble de domiciles numériques Cozy possédant l'information que nous voulons moyenner, mais seuls nous intéressent les Cozy appartenant à des personnes correspondant à une tranche d'âge précise.

Traditionnellement, un système de gestion de base de données centralisé possède toutes les informations nécessaires à l'exécution d'une requête. Or, ce n'est pas le cas ici : il est primordial que le système gérant la requête (Conductor) en sache le moins possible sur les individus. Cette étape est donc découpée en trois sous-tâches effectuées par trois serveurs sécurisés différents :

1. Traduction de la question pour anonymiser toute donnée personnelle utile à la sélection (Concept Indexor - CI).
2. Sélection des Cozy qui peuvent répondre à la requête (Target Finder - TF).
3. Récupération des données chiffrées et transmission à un serveur de calcul (Target - T).

Découper le processus de requêtage en autant de sous-étapes permet d'acheminer les données personnelles sans jamais révéler les données et l'identité des domiciles numériques concernés par le calcul. La donnée est transmise temporairement à l'intérieur d'un serveur de calcul (Data Aggregator - DA), mais n'est jamais stockée. Ne ressort de cette succession de boîtes noires qu'un résultat qui sera supposé reposer sur suffisamment d'individus pour n'en trahir aucun.

De plus, chaque sous-tâche (CI, TF, T, DA) peut-être divisée et menée par différents serveurs. Cette division est notamment utile pour DA afin de réduire le nombre de données que chaque serveur DA reçoit. Ainsi, nous pouvons réduire le risque d'attaque statistique (étude des données pour en déduire des informations sur la provenance de ces données) et nous pouvons réduire la durée de la requête.

Une intelligence artificielle bâtie sur le partage

La requête de l'exemple ci-dessus est relativement simple mais permet d'illustrer comment récupérer de l'information agrégée de manière sécurisée. Tout l'intérêt, ensuite, est de transposer ce protocole à l'intelligence artificielle. Au lieu de calculer une moyenne sur une unique information, nous pouvons entraîner un modèle sur un plus grand nombre d'éléments (e.g. rythmes cardiaque à différentes périodes, âge, sexe, indicateurs de l'activité sportive, etc).

Ce protocole permet d'envisager un entraînement d'une intelligence artificielle qui ne transgresserait pas la vie privée. Il ouvre la porte à des intelligences artificielles reposant sur des données plus privées pour des problématiques servants d'autant plus l'intérêt commun. Grâce à l'Internet des objets, grâce aux domiciles numériques, grâce au protocole DISPERS, il est envisageable d'étudier tout un nouveau jeu de données et repousser de nouvelles barrières, notamment dans le cadre de la recherche médicale.

Le papa d'Internet, Sir Tim Berners-Lee, plaide pour un Internet décentralisé. Un Internet qui ne tournerait plus autour des géants, un Internet neutre où tous les utilisateurs sont égaux, où chacun reçoit ou transmet du contenu en restant maître de ses données. Selon Sir Tim Berners-Lee, c'est la recherche perpétuelle d'une optimisation des rémunérations publicitaires qui est la cause des déboires d'Internet. Ce qu'il voyait comme un moyen de communiquer et de collaborer tout autour du globe est devenu un puissant outil de manipulation.

Le système est en train d'échouer [...] Il ne remplit plus son rôle d'aider l'humanité à promouvoir la vérité et la démocratie. ([Tim Berners Lee - The Guardian](#))

L'intelligence artificielle a sa part de responsabilité. Elle est le moyen d'optimiser le temps de cerveau disponible de chaque utilisateur pour générer un revenu maximal, ou pour concevoir des outils de propagandes remarquablement puissants. Le seconde est qu'elle a conduit, pour son entraînement, à une collecte d'informations sans précédent sur les utilisateurs, menant à une réelle violation de la vie privée des internautes.

Comme [Capgemini qui a présenté il y a peu un rapport à ce sujet](#), nous croyons à

une intelligence artificielle éthique qui aidera l'humanité dans les enjeux d'aujourd'hui et de demain. C'est pourquoi Cozy Cloud travaille sur ces problématiques au sein de son équipe R&D. Il s'agit d'un chantier considérable mais dont les perspectives sont gigantesques et particulièrement excitantes.

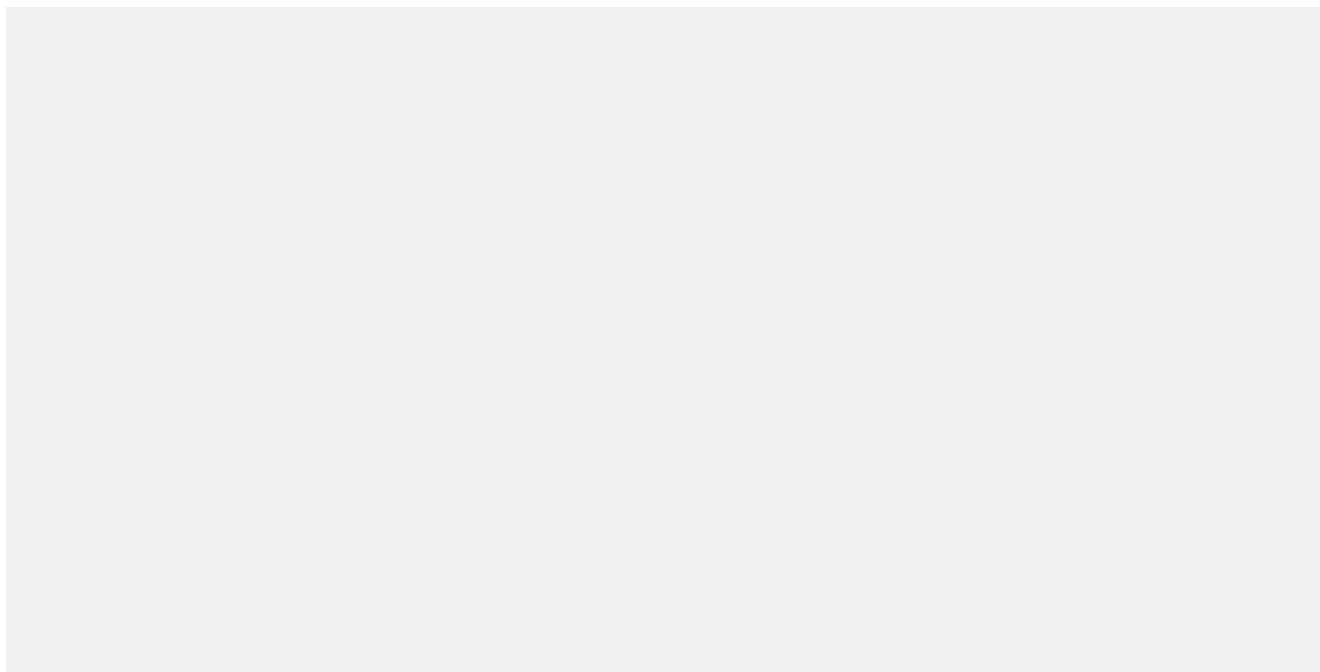
Pour aller plus loin, quelques lectures

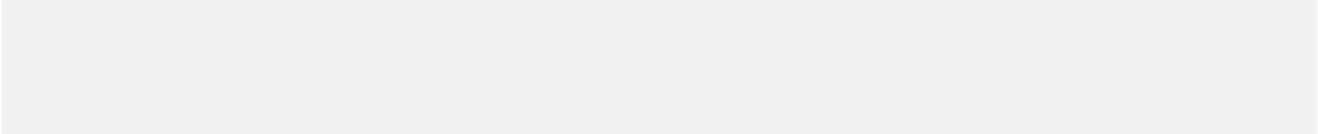
[FaceApp : pourquoi il faut s'en méfier](#) - Article paru en juillet 2019 - *Le Monde*
[Ethique de l'Intelligence Artificielle](#) - Etude réalisée par Cap Gemini - Juillet 2019
[Privacy-Preserving Queries on Highly Distributed Personal Data Management Systems](#) - *Julien Loudet, Luc Bouganim, Iulian Sandu Popa*
[SEP2P: Secure and Efficient P2P Personal Data Processing](#) - *Julien Loudet, Iulian Sandu Popa, Luc Bouganim*

Pour en discuter avec notre Responsable R&D

Paul Tran-Van : son [LinkedIn](#) ou [Twitter](#)

Rendez-vous sur [cozy.io](#) pour créer votre espace Cozy hébergé en France, respectueux de votre vie privée et gratuit jusqu'à 5 Go de stockage.

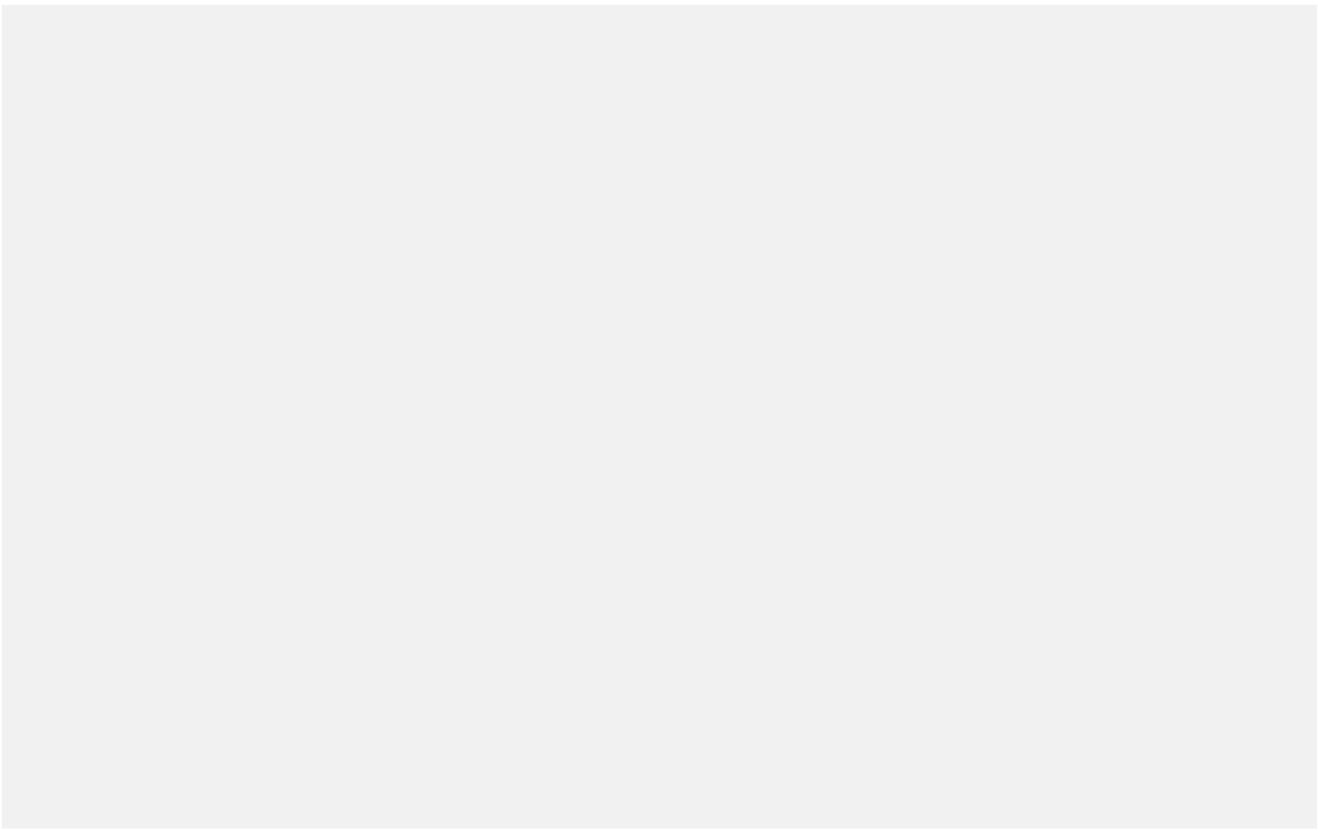




25 janv. 2018 • 2 min read

Jour 1 : Cozy Cloud lance Cozy

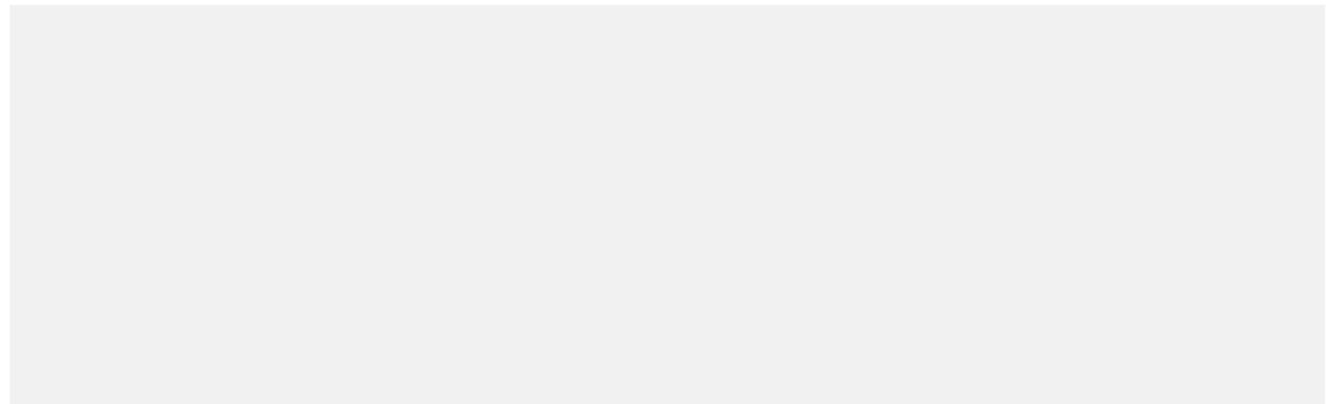
[read more →](#)

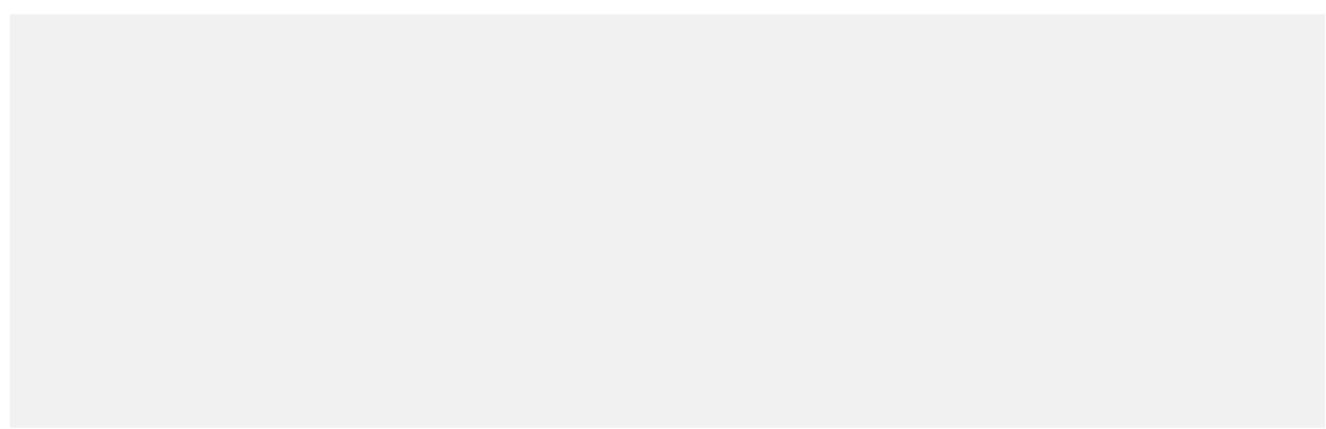


29 juil. 2022 • 5 min read ★

Quel est l'intérêt d'utiliser un logiciel open source ?

[read more →](#)





27 juin 2022 • 6 min read

Dans les coulisses de l'équipe Front End et Cozy Pass

[read more →](#)

Cozy Cloud © 2024

[cozy.io](#)

[Notes de version](#)

Powered by Ghost