



# Zoom sur : Les Privacy Enhancing Technologies (PETs)

**Date :** 21 janv. 2025

L'évolution récente des technologies de protection de la vie privée (ou Privacy Enhancing Technologies - ci-après les « PETs »), a ouvert de nouvelles perspectives permettant la création de technologies publicitaires efficaces renforçant les garanties de protection de la vie privée. Parmi ces technologies, on peut citer l'anonymisation, la pseudonymisation, l'homomorphic encryption, les trusted executive environments (TEEs), le zero-knowledge proof ou encore les outils de contrôle de l'utilisateur.

De manière plus générale, la notion de « PETs » est un terme générique désignant de multiples outils, technologies et techniques utilisés pour protéger les utilisateurs contre les cyberattaques, préserver leur vie privée, renforcer la protection de la vie privée et, dans un certain nombre de situations, minimiser la quantité de données personnelles traitées par des tiers, le tout sans limiter qualitativement la fonctionnalité des systèmes d'information en question.

Alors qu'au cours des deux dernières décennies, la publicité numérique est devenue de plus en plus centrée sur les données, des préoccupations en matière de protection de la vie privée ont été légitimement soulevées. La réponse d'un point de vue réglementaire à l'échelle européenne, fondée sur les deux piliers juridiques que sont la Directive ePrivacy et le Règlement RGPD, a conduit à un système basé sur le consentement qui, s'il a permis un certain niveau de protection, a également montré certaines limites en raison de la lassitude des utilisateurs à l'égard de ce système, phénomène désigné sous le terme de « fatigue du consentement ».

Dans ce contexte, The GAP encourage le secteur, les autorités et les législateurs à créer les conditions nécessaires pour que les PETs changent la donne dans le secteur de l'adtech. Dans cette optique, The GAP encourage les parties prenantes à travailler à une meilleure compréhension et sensibilisation au potentiel des PETs, au développement de bonnes pratiques, ainsi qu'à envisager les possibilités d'adaptation du cadre réglementaire, et en particulier de la Directive ePrivacy qui n'a pas évolué depuis plus de 20 ans, dans le but de promouvoir et d'encourager l'adoption des PETs dans le domaine de la publicité en ligne.

## De nombreux usages en dehors de la publicité digitale

Si les PETs suscitent un intérêt grandissant dans le domaine de la publicité digitale, elles sont déjà utilisées dans de nombreux autres secteurs d'activité, notamment :

**Transactions financières** : Les institutions financières, comme **Mastercard**, utilisent des PETs pour garantir la confidentialité des transactions et protéger la liberté des citoyens en leur permettant d'effectuer

des opérations avec des tiers de manière sécurisée. La **Société générale** est particulièrement impliquée dans le développement et l'utilisation des PETs, notamment à travers le projet DANIE qu'il a initié en 2020. Ce projet vise à permettre le partage et la collaboration autour des données clients tout en garantissant leur sécurité et leur anonymisation

**Gestion des données de test** : Les PETs permettent aux entreprises de contrôler l'accès aux données clients lors des phases de test et d'analyse d'applications, souvent réalisées par des tiers. Des entreprises comme **Cisco** utilisent ces technologies pour garantir la sécurité des données sensibles.

**Recherche scientifique et médicale** : Les PETs permettent de partager et d'analyser des données médicales sensibles tout en préservant la confidentialité des patients. Elles sont notamment utilisées pour des études sur les pandémies, la prédiction des taux d'infection et d'hospitalisation, ou encore la recherche sur les maladies rares.

**Protection de l'environnement et du développement durable** : Les PETs facilitent le partage de données environnementales sensibles, essentielles pour la production de rapports ESG (environnementaux, sociaux et de gouvernance). Elles permettent aux entreprises de partager ces informations tout en préservant leur confidentialité. C'est l'usage qu'en fait notamment **EDF** via les compteurs Linky.

**Lutte contre la criminalité financière** : Les PETs permettent le partage sécurisé de données financières entre différentes institutions, facilitant la détection et la prévention des fraudes et du blanchiment d'argent. Elles sont utilisées par des institutions comme la **Federal Reserve Bank** aux Etats-Unis.

## L'émergence des PETs dans le secteur de l'adtech

---

**La publicité numérique.** La publicité numérique consiste à promouvoir des produits ou des services par le biais de canaux numériques tels que les sites web, les réseaux sociaux, les moteurs de recherche et les applications mobiles.

Aux origines de la publicité numérique, tout espace publicitaire était obtenu directement auprès des éditeurs. Désormais, avec l'augmentation du nombre d'éditeurs commercialisant des espaces publicitaires, la publicité programmatique a finalement commencé à remplacer les réseaux publicitaires en tant que moyen automatisé d'achat et de vente d'espaces publicitaires numériques sur plusieurs sites web et éditeurs en temps réel.

**Publicité contextuelle et publicité personnalisée.** Historiquement, les deux principales approches de l'affichage publicitaire numérique sont les suivantes : (i) la publicité contextuelle qui s'adapte au contenu vu en temps réel par l'utilisateur, sans s'appuyer sur des informations préalablement collectées, et (ii) la publicité personnalisée (comportementale) qui s'appuie sur les centres d'intérêt de l'utilisateur pour afficher les publicités les plus pertinentes, déterminées à l'aide de divers outils de suivi. Parmi les nombreux outils de suivi, les plus répandus historiquement sont :

- **Cookies** : Fichiers stockés sur un appareil pour mémoriser les utilisateurs et leurs interactions. La synchronisation des cookies associe les données collectées à des identifiants centraux, facilitant le suivi publicitaire et augmentant le risque de réidentification.
- **Tracking pixels** : Liens invisibles intégrés dans des contenus, établissant une communication non sollicitée entre le client et l'hôte, contribuant au suivi des utilisateurs.
- **Device fingerprinting** : Combinaison d'attributs de l'appareil ou du navigateur pour créer un identifiant unique, permettant un suivi persistant avec un risque de réidentification.

**Préoccupations en matière de protection de la vie privée.** Au cours des dernières décennies, la publicité numérique est devenue un secteur de plus en plus centré sur les données. Les données collectées sur les utilisateurs comprennent des données démographiques, d'intérêt, d'intention, de localisation et de mesure (impressions, engagement, conversion). Elles sont utilisées pour cibler et mesurer les campagnes publicitaires et sont parfois liées à des identifiants communs qui permettent aux entreprises de dresser un tableau du comportement d'un individu sur les sites, les applications, les plateformes et les appareils. Au fur et à mesure que le traitement des données personnelles augmentait, la société a pris conscience des enjeux associés en termes de garantie de la vie privée. Parallèlement, les législateurs et les autorités chargées de faire respecter la loi ont renforcé les droits des individus en matière de protection de la vie privée. Dans l'Union européenne, la Directive ePrivacy de 2002 et le RGPD de 2016 ont constitué la base du cadre juridique visant à protéger la vie privée et les données à caractère personnel des consommateurs de l'Union européenne.

**Importance du secteur et sensibilisation à la protection de la vie privée.** Depuis l'apparition de la première bannière publicitaire en ligne en 1994, l'industrie mondiale est passée d'environ 99 millions d'euros en 1995 à 357 milliards d'euros en 2021. Cette croissance a notamment permis à un grand nombre d'éditeurs de créer de nouvelles sources de revenus et de favoriser un internet plus diversifié et centré sur le contenu, à commencer par le journalisme en ligne. Au cours de la dernière décennie, les principaux acteurs du secteur de la publicité numérique ont pris des mesures importantes pour limiter l'accès aux données liées à la publicité. Apple, en particulier, ont restreint le suivi des tiers sur leurs plateformes. De nombreux acteurs de la publicité en ligne, notamment au sein d'organisations interprofessionnelles, ont par ailleurs contribué au développement de standards visant à trouver le bon équilibre entre utilité et protection des données.

**Émergence des PETs appliquées à la publicité en ligne.** L'évolution récente des PETs, en particulier dans le domaine de la publicité en ligne, a ouvert de nouvelles perspectives pour développer des technologies publicitaires efficaces réduisant les risques pour les droits et libertés liés aux activités de traitement des données à caractère personnel. Jusqu'à présent, les principales parties prenantes observent que les principaux obstacles à l'adoption des PETs sont : le manque de compréhension et de sensibilisation au potentiel des PETs, l'absence de meilleures pratiques dans le secteur et le manque d'orientations officielles et de lignes directrices de la part des législateurs ou des autorités.

**Possibilité d'encourager le développement des PETs dans la publicité en ligne.** Les acteurs du secteur, les autorités et les législateurs ont la possibilité de travailler ensemble pour créer un nouveau cadre réglementaire, de nouvelles normes et de meilleures pratiques afin de promouvoir et d'encourager l'adoption des PETs dans la publicité en ligne.

## Impact positif des PETs sur la protection des données personnelles

---

Depuis de nombreuses années, on s'accorde de plus en plus à penser que les PETs peuvent avoir un impact positif sur la protection des données à caractère personnel, en particulier dans le secteur de la publicité en ligne.

Inspiré de la taxonomie établie par la **proposition de l'Agence de l'Union européenne pour la cybersécurité (ENISA)**, le tableau ci-dessous présente l'impact de différents types de technologies de l'information et de la communication sur un ensemble de principes découlant de la Directive ePrivacy et du RGPD.

		Minimisation	Finalité & conservation limitée	Intégrité et conf. (sécurité)	Transparence & maîtrise par l'Utilisateur Final
Pseudonymisation et Anonymisation	Pseudonymisation	x	x	x	
	(k-anonymity & differential privacy)		x	x	
Occultation des données et calculs préservant la vie privée	Homomorphic Encryption		x	x	
	Secure MPC	x	x	x	
	TEEs		x	x	
	Private Information Retrieval	x		x	
	Synthetic Data	x	x	x	
Accès, communication et conservation	End-to-end Encryption		x	x	
	Proxy & Onion Routing	x	x	x	
	Privacy Preserving Storage		x	x	
	Attribute Based Credentials	x	x	x	
	ZKPs	x	x	x	
Transparence, intervention et outils de contrôle de l'utilisateur		x	x	x	x

## Exemples de cas d'usage d'utilisation des PETs dans le secteur de l'adtech et autres

- **Les PETs reposant sur la pseudonymisation**

Par exemple, à des fins statistiques, **Spotify** partage des informations sur les utilisateurs, mais uniquement sous forme pseudonymisée. Plus concrètement, les données sont identifiées par un code plutôt que par le nom de l'utilisateur ou toute autre information permettant d'identifier directement l'utilisateur.

- **Les PETs reposant sur l'anonymisation** Récemment, le navigateur web **Brave** a introduit de nouvelles garanties pour ses utilisateurs, basées sur le respect différentiel de la vie privée. Il permet à la partie adtech intéressée d'obtenir des informations utiles sur les réactions d'une population à l'égard d'un produit sans rien apprendre sur les choix des individus au sein de cette population.

- **Les PETs reposant sur les environnements d'exécution de confiance (TEEs) :** En 2024, **Mozilla** a acquis Anonym, une infrastructure adtech axée sur l'amélioration des mesures de protection de la vie privée pour les données communément partagées entre les annonceurs et les réseaux publicitaires. Un élément clé de ce processus est l'endroit où ces données sont envoyées et stockées. Ainsi, au lieu que les annonceurs et les réseaux publicitaires partagent les données personnelles des utilisateurs entre eux, augmentant ainsi le risque pour les utilisateurs à chaque fois qu'un partage a lieu, Mozilla les crypte et les envoie à un TEE. Cette technique permet encore d'obtenir des informations et de la valeur à partir des données sans permettre le développement de profils comportementaux intersites basés sur des données au niveau de l'utilisateur. **Google** a mis au point une technologie nommée confidential matching offrant aux entreprises de nouvelles façons d'utiliser leurs données propriétaires pour atteindre les clients et mesurer l'impact de leurs campagnes publicitaires numériques. La combinaison des TEEs et du chiffrement de données permet d'isoler des données pendant leur traitement afin que personne, y compris Google, ne puisse y accéder en cours de traitement

- **Les PETs reposant sur la technologie du *Private Information Retrieval* (PIR) :** Parmi les développements intégrant le PIR, **AdVeil** est un écosystème privé de publicité ciblée construit autour d'un réseau publicitaire non fiable qui cible des publicités pertinentes pour les utilisateurs sans connaître aucune des informations personnelles de ces derniers. Concrètement, si la partie adtech intéressée prend connaissance des interactions publicitaires, elle ne sait pas quels sont les utilisateurs qui les ont générées.