

Google Analytics et transferts de données : comment mettre son outil de mesure d'audience en conformité avec le RGPD ?

07 juin 2022

Le 10 février 2022, la CNIL, après un processus de coopération avec ses homologues européens, a mis en demeure plusieurs organismes utilisant Google Analytics en raison des transferts illégaux de données vers les États-Unis. L'utilisation d'un proxy correctement configuré peut, cependant, constituer une solution opérationnelle pour limiter les risques pour les personnes.

La Cour de justice de l'Union européenne (CJUE), [dans son arrêt du 16 juillet 2020](#), a invalidé le *Privacy Shield*, dispositif qui permettait un encadrement des [transferts de données](#) personnelles entre l'Union européenne et les États-Unis. La législation états-unienne n'offre, en effet, pas de garanties suffisantes face au risque d'accès par les autorités, notamment les services de renseignement, aux données personnelles de résidents européens.

À la suite de cet arrêt, la CNIL avait été saisie de plusieurs plaintes, déposées par l'association NOYB, mettant en cause l'utilisation par des sociétés françaises de l'outil de mesure d'audience des sites web Google Analytics, édité aux États-Unis. Statuant sur ces plaintes, la CNIL a estimé qu'elles étaient fondées et a mis en demeure les sociétés en cause de se mettre en conformité.

Dans ces décisions ([dont une version anonymisée a été publiée le 10 février 2022](#)), la CNIL a estimé que l'utilisation de Google Analytics entraînait, en l'état, des transferts vers les États-Unis insuffisamment encadrés.

Comme rappelé dans la [FAQ de la CNIL à ce sujet](#), la simple mise en œuvre de clauses contractuelles types n'est pas suffisante pour utiliser Google Analytics en conformité avec le RGPD.

Une simple modification du paramétrage de l'outil est insuffisante

À la suite de ces mises en demeure, de nombreux acteurs ont cherché à identifier les paramètres et mesures techniques pouvant permettre de continuer à utiliser Google Analytics tout en respectant la vie privée des internautes.

Sur ce point, la seule modification du paramétrage des conditions de traitement de l'adresse IP ne suffit pas à satisfaire les exigences de la CJUE, notamment car ces dernières continuent à être transférées aux États-Unis. Une autre idée souvent avancée est celle du recours au « chiffrement » de l'identifiant généré par Google Analytics, ou bien du remplacement de celui-ci par un identifiant généré par l'opérateur du site. Toutefois, en pratique, cela n'apporte que peu ou pas de garanties supplémentaires contre une éventuelle réidentification des personnes concernées, principalement du fait de la persistance du traitement de l'adresse IP par Google.

La problématique fondamentale qui empêche ces mesures de répondre à la problématique de l'accès aux données par des autorités extra-européennes est celle du contact direct, par le biais d'une connexion HTTPS, entre le terminal de la personne et des serveurs gérés par Google.

Les requêtes qui en résultent permettent à ces serveurs d'obtenir l'adresse IP de l'internaute ainsi que de nombreuses informations sur son terminal. Celles-ci peuvent, de manière réaliste, permettre une réidentification de celui-ci et, en conséquence, l'accès à sa navigation sur l'ensemble des sites ayant recours à Google Analytics.

Seules des solutions permettant de **rompre ce contact entre le terminal et le serveur** peuvent répondre à cette problématique. Au-delà du cas de Google Analytics, ce type de solution pourra également permettre de concilier l'usage d'autres outils de mesure avec les règles du RGPD sur le transfert de données.

Une solution possible : la proxyfication

Au vu des critères évoqués précédemment, une solution possible est celle de l'utilisation d'un serveur mandataire (ou « *proxy* ») pour éviter tout contact direct entre le terminal de l'internaute et les serveurs de l'outil de mesure (donc en l'espèce de Google). Il faut cependant s'assurer que ce serveur **remplit un ensemble de critères** pour pouvoir considérer que cette mesure supplémentaire s'inscrit dans la ligne de ce qui est prévu par le CEPD dans [ses recommandations du 18 juin 2021](#). En effet, un tel dispositif correspondrait au cas d'usage de **la pseudonymisation avant export de données**.

Comme indiqué dans ces recommandations, un tel export n'est possible que si le responsable du traitement a établi, au moyen d'une analyse approfondie, **que les données personnelles pseudonymisées ne peuvent être attribuées à une personne physique identifiée ou identifiable**, même si elles sont recoupées avec d'autres informations.

Il s'agit donc, au-delà de la simple absence de requête depuis le terminal de l'utilisateur vers les serveurs de l'outil de mesure, de s'assurer que **l'ensemble des informations transmises ne permet en aucun cas une réidentification de la personne**, même en prenant en compte les moyens conséquents dont disposent les autorités susceptibles de vouloir procéder à une telle réidentification.

À noter

La mise en œuvre des mesures décrites ci-dessous peut se révéler coûteuse et complexe et ne permet pas toujours de répondre aux besoins opérationnels des professionnels. Pour éviter ces difficultés, il est également possible pour les professionnels de recourir à une solution ne réalisant pas de transferts de données personnelles en dehors de l'Union européenne.

Les mesures nécessaires à mettre en place pour que la proxyfication soit valable

Le serveur procédant à la proxyfication devra donc mettre en œuvre un ensemble de mesures permettant de limiter les données transférées. La CNIL considère, en principe, comme nécessaire :

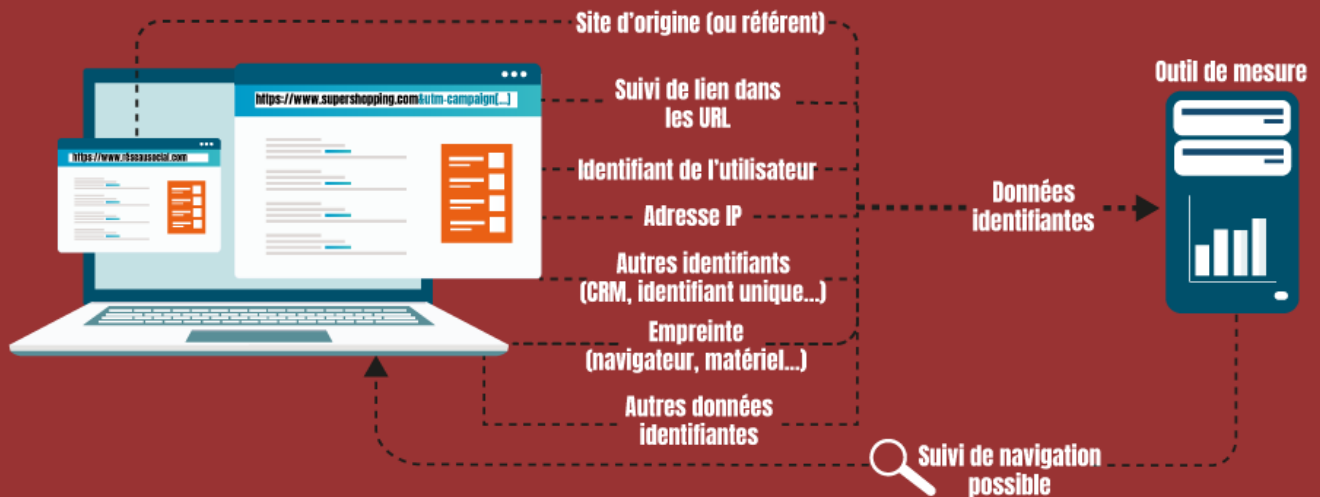
- **l'absence de transfert de l'adresse IP vers les serveurs de l'outil de mesure.** Si une localisation est transmise vers les serveurs de l'outil de mesure, celle-ci doit être opérée par le serveur proxy et le niveau de précision doit permettre de s'assurer que cette information ne permet pas une réidentification de la personne (par exemple en utilisant un maillage géographique assurant d'un nombre minimum d'internautes par cellule) ;
- **le remplacement de l'identifiant utilisateur par le serveur de proxyfication.** Pour assurer une pseudonymisation effective, l'algorithme effectuant le remplacement devrait assurer un niveau de collision suffisant (c'est-à-dire une probabilité suffisante que deux identifiants différents donnent un résultat identique après [hashage](#)) et comporter une composante temporelle variable (ajouter à la donnée hashée une valeur qui évolue avec le temps pour que le résultat du hashage ne soit pas toujours le même pour un même identifiant) ;
- **la suppression de l'information de site référent (ou « *referrer* ») externe au site ;**
- **la suppression de tout paramètre contenu dans les URL collectées** (par exemple les UTM, mais aussi les paramètres d'URL permettant le routage interne du site) ;
- **le retraitement des informations pouvant participer à la génération d'une empreinte (ou *fingerprint*)**, tels que les « *user-agent* », pour supprimer les configurations les plus rares pouvant mener à une réidentification ;
- **l'absence de toute collecte d'identifiant entre sites (*cross-site*) ou déterministe (CRM, [unique ID](#)) ;**
- **la suppression de toute autre donnée pouvant mener à une réidentification.**

Les conditions d'hébergement du proxy doivent également être adéquates

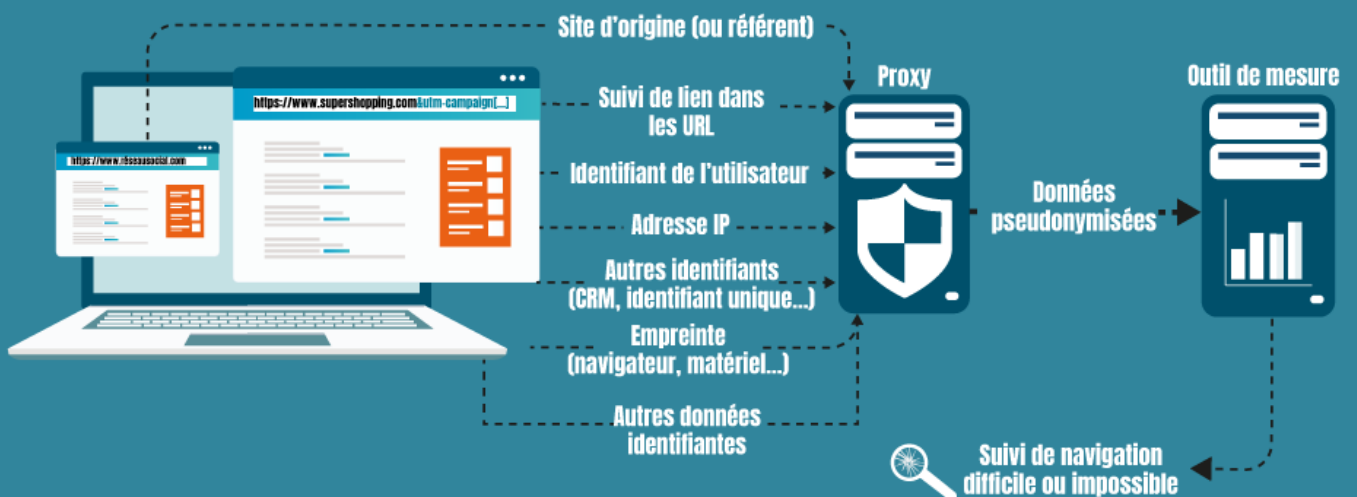
Le serveur de proxyfication devra aussi être hébergé dans des conditions permettant de garantir que les données qu'il sera amené à traiter ne seront pas transférées hors de l'Union européenne vers un pays n'assurant pas un niveau essentiellement équivalent à celui prévu dans l'Espace économique européen.

En tout état de cause, et conformément aux recommandations du CEPD, il reviendra aux responsables de traitement de procéder à une analyse sur ce point et de mettre en place les mesures nécessaires dans le cas où ils souhaitent utiliser ce type de solutions, ainsi que de vérifier le maintien de ces mesures dans le temps, au gré des évolutions des produits.

Statistiques sans proxyfication



Statistiques avec proxyfication



Texte reference

Pour approfondir

> [Cookies et autres traceurs : les règles à respecter](#)

> [Questions-réponses sur les mises en demeure de la CNIL concernant l'utilisation de Google Analytics](#)