Association Loisirs et culture

Éliminez les bannières « J'accepte » et les notifications des sites.

Jean Marie Herbaux

Table des matières

1. Préambule 2
2. RGPD, quatre lettres pour une histoire de cookies. 2
3. Collecte des données personnelles : de quoi s'agit-il ? 2
4. Un bestiaire complet pour vous traquer. 3
   a. Les pixels espions. 3
   b. Le code javascript fournis par des sociétés de publicités tierces. 3
   c. Les kits de développement logiciels ou SDK 3
   d. Les identifiants d'appareils. 3
5. Ls navigateurs déjà à la manœuvre 3
6. Comment éviter les messages de confirmation de la RGDD 3
   a. Méthode 1 : 3
      - Téléchargez "**I don't care about cookies**" (Firefox, Chrome, Edge) 3
   b. Méthode 2 : renforcer le blocage du pistage 4
   c. Méthode 3 : Utilisez la navigation privée. 4
7. Les demande de notifications, l'autre plaie du web 5

1. Préambule

Elles s'affichent sur la plupart des sites et vous demandent d'accepter ou de parcourir de nombreux réglages pour les désactiver. Ce sont les bannières de demande de RGPD ce fameux Règlement Général sur la Protection des Données qui empoisonne la vie de tous les internautes depuis plus de trois ans.
Le premier réflexe consiste à cliquer sur *J'accepte* si l'on souhaite accéder rapidement à un contenu. Dans cet article nous vous expliquons comment vous passer de cette contrainte et également comment mettre fin à un autre phénomène à la mode très agaçant, l'apparition de petits modules vous proposant d'ajouter des *notifications* en cas de nouveautés. Voici comment procéder.

2. RGPD, quatre lettres pour une histoire de cookies.

Promulgué en 2016 et mis en place en 2018 le R.G.P.D au sein de l'union européenne devait permettre de protéger les internautes de la collecte d'informations personnelles à leur insu. Une règlementation louable dans l'esprit, mais dont l'application est devenue une véritable contrainte pour l'utilisateur. Ainsi sur pratiquement tous les sites. dès que vous affichez la page Internet, un module se superpose et vous demande de faire un choix entre *Accepter* la collecte d'Informations ou bien la *Refuser*. Ce dernier bouton n'est disponible que dans de très rares cas.
A la place, dans 95 % de cas, on trouve un bouton beaucoup moins visible ou qui porte un nom peu significatif et qui permet d'accéder à une multitude d'options liées à la collecte de vos données personnelles.
Au final presque tout le monde accepte ces conditions. Cela revient donc à la pratique antérieure au RGPD avec cette contrainte supplémentaire ! c'est simplement ce qu'on appelle le consentement implicite, une pratique très courante à la limite de la légalité.

3. Collecte des données personnelles : de quoi s'agit-il ?

Pour récupérer des information sur vos comportements sur internet, les sites déposent sur votre ordinateur de petits fichiers baptisés *cookies*. Ce procédé est vieux comme les premiers sites web. il permet au site de vérifier la taille de votre écran pour adapter son contenu, votre système d'exploitation et votre navigateur pour vous permettre de bénéficier de certaines de ses fonctionnalités d'affichage, ou encore la date de votre dernière visite sur le site. Dans de très nombreux cas, cela permet aussi au site de savoir quelles informations vous ont plu lors de la dernière visite et le temps que vous avez passé sur le site et sur ses articles ou informations.
L'objectif est de vous fournir un contenu adapté à vos recherches mais pas uniquement car le cookie permet au site de *se faire rémunérer* en affichant des publicités adaptées aux gouts qu'il a relevé lors de vos séances de recherche.

Ainsi. vous avez certainement remarqué, si vous cherchez un produit précis, vous pouvez être certain que vous allez le voir s'afficher via des publicités sur des sites qui n'ont absolument aucun rapport. même si vous ne vous êtes jamais connecté à ces sites.
Attention, car il y a les cookies du site, mais aussi les cookies de sociétés tierces invitées par ce site. C'est le cas des régies publicitaires et en premier lieu de *Google*. Votre navigateur peut ainsi se trouver engorgé de plusieurs dizaines de cookies. Il faut savoir que certains cookies ont la peau plus dure que d'autres .

Il existe :

- des cookies de cession (valable le temps de la visite du site).
- des cookies de géolocalisation temporaires (valables jusqu'à 4 heures).
- des cookies persistants (valables 1 jour, 1 mois ou une année).

il faut savoir que les cookies n'ont pas véritablement vocation à améliorer la navigation. Même s'ils adaptent les contenus. Bien au contraire l'installation, la lecture et l'écriture des cookies représentent encore plus de la moitié du temps de chargement d'une page.

4. Un bestiaire complet pour vous traquer.

Les cookies ne sont pas seuls à s'inviter dans le navigateur en cas de clic sur *Accepter*. D'autres créatures qui leur sont liées ou qui fonctionnent de manière autonome servent aussi à traquer l'utilisateur dans ses pérégrinations sur le web.

a. Les pixels espions.

Les pixels (également appelés « balises web » , « gif » ou « bogues ») sont des images transparentes de la taille d'un pixel situées sur des pages web ou des messages. Ils permettent de savoir si vous avez ouvert ces pages web ou ces messages. Les pixels dépendent souvent des cookies pour fonctionner, donc la désactivation des coolies peut tes altérer. Mais même si vous désactivez tes cookies, les pixels peuvent détecter une visite de page web...

b. Le code javascript fournis par des sociétés de publicités tierces.

Le JavaScript est un langage de programmation. Il peut être utilisé pour mesurer la façon dont sous interagissez le site que vous visitez.

c. Les kits de développement logiciels ou SDK.

Les SDK sont des morceaux de code fournis par des sociétés de publicité tierces. Ils visent essentiellement les applications mobiles pour collecter et analyser certains appareils et les données des utilisateurs.

d. Les identifiants d'appareils.

Il s'agit en quelque sorte de la plaque d'immaculation de votre ordinateur Chaque ordinateur est identifié par les annonceurs de façon unique leur permettant de le reconnaitre.

5. Ls navigateurs déjà à la manœuvre

Si les messages relatifs à la RGPD sont agaçants pour tous, les navigateurs sont déjà à la manœuvre pour en atténuer la portée. Car pour inscrire des cookies et autre créatures vous traquant, il faut encore qu'ils soient autorisés par le navigateur il se trouve que, depuis quelques années, des navigateurs proposent une personnalisation poussée des cookies. Ainsi. depuis mars 2010. le navigateur web d'Appel safari propose aux utilisateurs la possibilité de ne plus être tracké par les sites web qu'ils visitent. Plus récemment la durée de vie des cookies a été limitée à 7 jours, contre 30 jours auparavant. Enfin. Google à son tour et a annoncé la suppression des cookies tiers sur son navigateur Chrome pour 2022.

6. Comment éviter les messages de confirmation de la RGDD

a. Méthode 1 :

- Téléchargez "I don't care about cookies" (Firefox, Chrome, Edge)

Voici une astuce que vous allez adorer II s'agit d'un petit greffon à ajouter à votre navigateur. Son nom signifie : « Je me fiche des cookies » Sa mission est d'éviter d'afficher les bannières de demande de validation ou de refus de La RGPD. Son inconvénient c'est qu'en contrepartie de la suppression de

la bannière, cette extension accepte tous les cookies proposés. C'est lui qui clique sur *Accepter* à votre place.

Avec google chrome :

À partir du navigateur saisissez dans la barre d'adresse :
https://chrome.google.com/webstore/category/extensions
pressez entrée. Vous voici dans la bibliothèques des extensions pour le navigateur google chrome.
En haut à gauche dans l'outil de recherche saisissez « *I don't care about cookies* ». Il est probable que le navigateur affiche le nom de l'extension en premier dans sa liste de propositions.
Cliquez sur la fiche puis sur *Ajouter à Chrome* et encore *Ajouter l'extension*, dans le module qui apparait une fois le greffon ajouté, il apparait en haut à droite du navigateur.
Il n'y a pas vraiment de réglage à effectuer le module est directement opérationnel. En revanche. si vous souhaitez l'éteindre, il faut cliquer en haut à droite sur les trois petits points puis sur plus d'outils et dans le sous menu *Extensions*.
Dans la fenêtre qui s'affiche, vous pouvez *activer* ou *désactiver* les différents modules en sous contentent de cliquer sur le petit interrupteur disponible.

Arec Microsoft Edge.

La nouvelle version du navigateur pour Windows 10 est similaire à Google Chrome. Vous pouvez donc effectuer la même opération. Il faudra seulement cliquer sur le bouton *autoriser* dans le message d'avertissement qui va s'afficher.
Il n'y a pas vraiment de réglage à effectuer le module est directement opérationnel. En revanche. si vous désirez l'étendre. il faut cliquer en haut à droite sur les trois petits puis sur plus d'outils et dans le sous menu *Extensions*.
Dans la fenêtre qui s'affiche. vous pouvez *active* ou *désactiver* les différents modules en vous contentant de cliquer sur le petit Interrupteur disponible.

b. Méthode 2 : renforcer le blocage du pistage

Pour limiter les risques de pistage. vous pouvez réaliser quelques réglages simples depuis votre navigateur

Avec Google Chrome :

Cliquez sur les trois points superposés en haut, à droite et choisissez *Paramètres* dans le menu.
Faites défiler la page et en bas cliquez sur *Paramètres avancés*.
Rendez-vous dans la rubrique confidentialité et Sécurité.
Cliquez sur l'option *Cookies et autres données de site*.
Dans le nouvel affichage sélectionnez *Bloquer les cookies tiers* puis cliquez sur l'interrupteur à droite de *Effacer les cookies et les données du site en quittant Chrome*. L'interrupteur vire au bleu. Vérifiez que celui de la ligne du dessous est également bleu.
En dessous de envoyer au site web un signal *Ne pas me pister* Indiquant que vous ne souhaitez pas être pisté. sélectionnez *Toujours*.

Microsoft Edge :

Cliquez en haut à droite sur les trois points puis sur Paramètres.
Dans la page, à partir de la colonne de gauche, sélectionnez *Cookies et autorisations du site*
Dans la partie principale, activez l'interrupteur à droite de *Bloquer les cookies tiers*.

c. Méthode 3 : Utilisez la navigation privée.

La navigation privée est une solution simple pour ne plus être ennuyé avec ces histoires de cookies. Quel que soit le navigateur, il est possible de l'ouvrir en mode privé par défaut. Concrètement quand

vous activez ce mode de navigation. plusieurs informations habituellement enregistrées ne sont pas conservées.
Ainsi, en navigation privée les sites ne peuvent pas collecter votre *historique*, vos *recherches* ou des *fichiers temporaires* sur votre ordinateur. Les cookies ne fonctionnent pas et les *publicités* ne peuvent pas sous cibler.
Tous ces éléments, bien qu'ils soient conservés pendant votre navigation sont supprimés dès que vous fermez votre navigateur.
Attention :
Prive ne signifie pas anonyme et Invisible sur Internet. Les sites peuvent toujours vous identifier grâce à votre *adresse IP* c'est-à-dire l'équivalent du numéro de téléphone de votre point d'accès à Internet. De même en navigation. Enfin votre fournisseur d'accès Internet (FAI) peut toujours connaître vos comportements puisque les données transitent par lui.

Exemple d'atout de le navigation privée.
Vous souhaitez acheter un billet d'avion. Lorsque vous consultez le même site le lendemain, vous constatez que les tarifs du vol ont augmenté. Et de même encore le surlendemain. Vous réservez le billet immédiatement et vous avez la sensation d'avoir fait une bonne affaire malgré tout. Si vous utilisez votre téléphone en 4G, vous vous rendrez compte pourtant que le tarif est toujours celui du départ.
Pourquoi ? Le site à compris grâce à votre adresse IP que sous vérifiez régulièrement les tarifs et a analysé votre comportement. Pour vous Inciter à accélérer la manœuvre le site a artificiellement augmenté le cout affiché. En utilisant la navigation privée, vous faites croire au site que c'est votre première visite. Sachez que cette pratique est désormais illégale en Europe. En revanche, la question peut se poser pour certaines compagnies aériennes ou sites hors d'Europe

Avec Chrome
Cliquez en haut à droite sur les trois points puis sur Nouvel onglet de navigation privée. Une Interface sombre permet de vous naviguez bien de façon privée. Chrome n'enregistrera pas notre historique ni les cookies. ni non plus les données du site.
Comment obliger Chrome à démarrer en mode privé.
Faites un clic droit sur l'icône du raccourci du navigateur (sur Google Chrome si vous le faite depuis un raccourci épinglé la barre des taches) et cliquez sur Privé.

Avec Microsoft Edge.
Cliquez en haut à droite sur les trois petits points et choisissez Nouvelle fenêtre in private.

7. Les demande de notifications, l'autre plaie du web
En plus des sollicitations pour accepter en l'état ou refuser les cookies et autres traqueurs, il y a aussi ces petits modules qui s'affichent en haut de la page de la plupart des sites. Leur demande : *accepter* ou *bloquer* l'affichage de *notifications*. Cela permet aux sites d'envoyer de petits messages en cas de nouveautés. Ces notifications peuvent rapidement être envahissantes. Je vous conseille de les refuser en cliquant sur le bouton *Bloquer*, disponible. Mais il y a mieux à faire, interdire tout simplement cet affichage.

Avec Google Chrome :
Cliquez sur les trois petits points superposés puis sur *Paramètres*.
Dans la colonne de gauche, cliquez sur *Confidentialité et sécurité*. Sous *Notifications*, désactivez l'interrupteur.

Avec Microsoft Edge
Cliquez sur les trois points à droite, puis *Paramètres*. Sélectionnez *Cookies et autorisations de site*.

Faites défiler les options pour attendre la rubrique *Autorisations des Sites*. Cherchez *Notifications*, cliquez dessus. Laissez *Me demander avant d'envoler désactivé*.