Cookies : passé, présent et « no future »

Denise Tripalo-Cavero
Senior AdOps Manager
mediatonic sa

Fameux cookies, qui sous l'œil suspicieux et inquiet de l'internaute et des acteurs réglementaires du marché publicitaire digital animent les discussions les plus vives relatives au respect de la vie privée. Le cookie ; une espèce certainement pas rare, d'ailleurs quasiment omniprésente dans le monde de la publicité digitale, mais au goût de plus en plus amer pour la grande partie des internautes. Une espèce menacée dans un monde de « privacy-first », voie de disparition programmée. Le 3rd party tracking, ces cookies digitaux que (plus) personne n'aime : tour d'horizon.

C'est quoi déjà un cookie ?

En très simplifié, les cookies sont des fichiers de récolte d'information utilisés par les navigateurs web et qui ont pour tâche le stockage, l'exploitation et le partage des informations relatives à l'internaute. Une distinction capitale est à faire entre des cookies de première partie (1st party tracking) et des cookies tiers (3rd party tracking). La différence réside dans le type d'informations stockées, l'usage que l'on fait de ces informations et pour finir et surtout le partage de ces informations.

L'utilisation de cookies première partie est liée au côté pratique de la navigation sur Internet. Par exemple, lorsqu'un internaute arrive sur un site web – ne fait aucune action sur le site – part puis revient dans une autre session, le site ne sait plus forcément qui est cet internaute. Si cet internaute place maintenant un produit dans la corbeille – c'est là qu'il y a dépôt de cookie dans le navigateur – repart et revient dans une autre session, le produit sera toujours présent dans le panier. Tant que l'échange entre l'utilisateur et le navigateur se fait avec le même site web ou la même application, il s'agit de cookie première partie. Cela permet d'offrir une meilleure expérience de navigation à l'utilisateur sur un site web qu'il visite souvent.

L'utilisation des cookies tiers a permis la mise en place d'activités essentielles au marketing digital.

Dans le cas de cookies tiers, prenons l'exemple d'un internaute qui se rend sur un site de comparaison d'assurance maladie. Au cours des jours qui suivent, quels que soient les sites qu'il visite, il est exposé à de la publicité dans le domaine de l'assurance maladie. Ces annonces qui lui sont proposées, ne sont pas générées par le site web initial qu'il a visité, mais par des acteurs tiers qui identifient cet internaute grâce aux cookies tiers chargés sur son navigateur sur le site initial. Dans cet échange qui n'est plus entre l'utilisateur et le site initial, dès le moment qu'il y a partage de l'information au

sujet d'un internaute entre un site visité et un prestataire tiers, nous avons affaire à des cookies de tierce partie.

Les mécanismes fondamentaux de la publicité numérique reposent principalement sur l'utilisation des cookies tiers. Ces derniers ont permis la mise en place des activités essentielles au marketing digital, à savoir :

- Le ciblage : identifier l'internaute et pouvoir l'atteindre, y compris via le retargeting
- Le capping : adresser les messages à une fréquence contrôlée
- L'attribution : la possibilité de mesurer la performance des activités digitales

Etat des lieux et fond du problème

Concrètement, il n'y a pas de réelle problématique avec les 1st party cookies, c'est à dire les cookies utilisés par les sites web pour collecter des informations sur les utilisateurs qui ont choisi et sont d'accord d'interagir avec ces derniers.

A l'inverse, les cookies 3rd party sont eux identifiés comme non respectueux de la vie privée des internautes, car ne répondent pas aux normes légales en vigueur et à la réglementation GDPR et sont condamnés à la disparition. Bien que des discussions à ce sujet ne soient pas encore totalement résolues dans certains pays de l'UE et que les exigences en matière de respect de l'ePrivacy ne soient pas de la même rigidité partout, comme notamment en Suisse, les cookies tiers ont déjà été exclus des navigateurs Firefox et Safari depuis plus de deux années. Les événements se sont surtout accélérés au début de l'année passée, lorsque le monde de la publicité numérique emmagasine l'annonce choc faite par le géant Google : ce dernier s'engage lui aussi à éradiquer les 3rd party cookies de son navigateur Chrome, leader mondial de l'utilisation d'Internet à hauteur de 65% de part du marché. Google se donne deux années pour mettre en pratique cette nouvelle politique, le compte à rebours est lancé.

Le respect de la vie privée des internautes a parlé et a gagné, comme réponse aux réglementations sur ce dernier, les cookies

tiers – entraînant les activités essentielles au marketing digital classique – disparaissent du secteur de la publicité.

Démystification nécessaire du problème

Bien que la perspective d'un futur dénué de cookies ait pu faire trembler le milieu du marketing digital et semble soulever des craintes quant à la continuité de certaines activités online, il semble également clair que l'arrêt de ces activités n'est pas réel et encore moins envisageable. Selon l'IAB, cela se confirme du côté des internautes : très sceptiques quant à l'utilisation de leurs données sur Internet, ils affirment tout de même à hauteur de 71%, préférer de la publicité ciblée en fonction de leurs intérêts et habitudes de shopping. Et 75% d'entre eux déclarent même préférer moins d'annonces publicitaires, mais plus pertinentes, à comprendre plus ciblées.

L'industrie digitale doit s'assurer de trouver des solutions pérennes et conformes pour éviter de se reconfronter au manque de confiance des internautes.

Les acteurs de l'industrie digitale, qu'il s'agisse d'annonceurs, d'agences publicitaires, des éditeurs ou encore des compagnies AdTech, connaissaient l'imminence du cookie-less, qui n'est en aucun cas une grande nouveauté. C'est une problématique à laquelle l'écosystème est confronté depuis deux années, pour rappel avec la compensation du manque à gagner sur les navigateurs Safari et Firefox qui ont déjà supprimé les cookies tiers, mais également avec les recherches de solutions pour les environnements mobiles et in-app exempts, pour la plupart, de cookies 3rd party.

Dès lors, annonceurs, éditeurs et compagnies AdTech sont conscients depuis un certain temps de la nécessité de proposer des alternatives, mais aussi du besoin de se réinventer, c'est-à-dire développer et créer de nouvelles façons de faire dans l'univers digital post-cookie. Mais ce que l'industrie digitale doit surtout faire est de s'assurer de trouver des solutions pérennes et conformes, qui vont éviter de se reconfronter aux problèmes de confiance de la part des internautes qui ont été amenés par les cookies tiers.

Les alternatives et leurs limites

Pour rapide rappel et pour un cadre dans cette approche, le marché doit proposer des solutions qui ne s'appuient pas sur l'utilisation des 3rd party cookies ou en copiant leur fonctionnement. Comme c'était le cas par exemple du Fingerprinting – qui permettait d'identifier et suivre, non un internaute, mais un device au travers de son utilisation d'Internet. Alternative qui est illégale au sens de la réglementation GDPR en omettant d'obtenir préalablement au pistage le consentement explicite de l'internaute.

L'utilisation du 3rd party tracking ne concerne cependant pas toutes les activités du marketing digital et n'est pas une nécessité absolue. A ce stade, on évoque souvent les ciblages contextuel et sémantique qui s'offrent comme alternatives au pistage via les cookies. Le ciblage contextuel permet de diffuser de la publicité en fonction des intérêts supposé d'un internaute. Par exemple, un annonceur bancaire qui déciderait d'être présent sur des sites dans le domaine de la finance. Un ciblage sémantique va pouvoir toucher des internautes qui s'intéressent à un thème particulier en leur proposant de la publicité en fonction de la présence de mots-clés de la page sur laquelle ils se trouvent. Dans ces deux alternatives, les limites sont claires ; se concentrer uniquement sur ce type de ciblage représente un retour en arrière dans l'éventail de possibilités acquises grâce à l'intelligence artificielle ou de l'apprentissage automatique en matière de création de segments. Toutes les visites d'un certain site ou tous les lecteurs d'un certain contenu ne font

pas forcément partie du groupe cible, ce qui entraîne une dispersion des investissements.

D'autres alternatives ont vu le jour sur le marché de la publicité digitale. Le géant Google, s'est lui-même essayé à cet exercice en proposant son système FLoC (Federated Learning of Cohorts). Avec cette technologie, un algorithme analyse les utilisateurs, leurs habitudes et leurs préférences, et les regroupe en segments anonymisés qui sont des groupes d'internautes susceptibles de recevoir les mêmes publicités parce que partageant des caractéristiques communes. Cependant, Google ne semble pas répondre aux exigences de consentement centrales pour la réglementation GDPR. La création de cohortes ne pouvant fonctionner sans l'enregistrement des données des internautes, Google qui ne possède pas et ne contrôle pas les identifiants nécessaires, a stoppé ce printemps tous les tests prévus pour mener à bien le projet.

Les solutions clé déjà existantes

Parmi les premiers pointés du doigt dans la guerre aux cookies, les compagnies AdTech, avec plus précisément leurs technologies liées au real-time-bidding (RTB) – achats programmatiques automatisés sur modèle d'enchère – s'avèrent des pionniers en matière d'adaptations et changements du savoir-faire, sans l'utilisation du 3rd party tracking. Déjà mis à mal courant été 2019 lorsque le bureau britannique de régulation des données personnelles – ICO, Information Commissionner's Office – publie un papier qui exprime ses inquiétudes d'atteinte aux droits et libertés des individus dans le cadre de l'industrie RTB. Particulièrement en cause, certaines compagnies AdTech qui n'obtiendraient pas explicitement le consentement des internautes lorsqu'ils exposent des annonces publicitaires aux internautes. L'industrie AdTech se défend à ce moment-là en assurant qu'il n'y a aucune donnée personnelle identifiable dans leur écosystème. Et assure même que l'amélioration du contrôle consommateur ne peut entraîner que des changements significatifs, mais positifs. Encore une fois, il va de soi que la mise en péril de l'univers AdTech, que ce soit niveau RTB, ciblage ou encore attribution, n'est pas une option.

Avec notamment des réponses liées à la problématique du cross-device – la capacité de reconnaître et de suivre un internaute d'un terminal d'accès à un autre, le plus souvent de son smartphone à son ordinateur en passant par la tablette – les compagnies AdTech

se sont concentrées sur les technologies basées sur les cookies 1st party, qui pour rappel n'entrent pas dans le champ du problème de cookies tiers. Les cookies de première partie – informations récoltées inscrites dans le cookie local sur le domaine de l'éditeur ou un domaine partagé avec certains éditeurs – sont conformes à la réglementation GDPR, car sont situés et gérés du côté des éditeurs. Par définition, ils répondent à la protection de la vie privée des internautes, car sont, à priori, soumis au consentement du l'utilisateur dès son arrivée sur le site.

Les éditeurs également responsables du consentement s'organisent déjà en groupement d'éditeurs.

Cette solution, qui est une réponse respectueuse de la réglementation sur la vie privée, en est également une pour l'ensemble du marché, d'où découlent deux nouveaux chapitres fondamentaux qui s'ouvrent dans l'ère post-cookies ; l'exploitation des 1st party et la gestion du consentement.

Vers un univers « privacy-friendly »

Du côté des compagnies AdTech, on s'appuie sur les cookies de première partie pour créer des identifiants d'utilisateurs. On va parler de 1st party IDs qui existent principalement sous deux formes ; les IDs basés sur un login – les internautes qui saisissent leurs identifiants de connexion pour l'utilisation d'un site ou d'un service – et les 1st party server cookies – les cookies première partie placés sur les navigateurs par les éditeurs. Bien que chaque fournisseur d'ID 1st party ait sa propre façon technique de fonctionner, ils ont en commun le même objectif, c'est-à-dire partager l'identifiant de l'internaute concerné, fourni sous forme cryptée, avec les systèmes impliqués dans la publicité. De cette façon, à la place des cookies tiers, les identifiants 1st party sont utilisés pour faire correspondre les données des systèmes et des plateformes Internet.

Du côté des éditeurs, responsables du consentement des internautes, on s'organise également avec notamment des groupements d'éditeurs qui ont déjà été mis en place – pour citer les plus grands NetID, BritePool, LiveRamp, Unified ID, Ozone ou encore OneLog, le groupement suisse entre Ringier et le TX Group. Par exemple, un utilisateur qui visite le site du Huffington Post, sera d'abord redirigé vers une CMP (Consent Management Platform) externe qui va collecter son consentement et une fois obtenu pouvoir le partager avec les sites partenaires de Verizon Media, éditeur du site, mais va également permettre de réguler, surveiller et de tracer les différents fournisseurs qui ont des accès aux données des utilisateurs particuliers.

Certains acteurs du marché, comme ID5 ou AdForm, vont même plus loin en proposant des identifiants universels qui fonctionnent de la manière suivante : lorsqu'un utilisateur arrive sur un site web, l'éditeur le redirige automatiquement sur un domaine partagé où le consentement est demandé et, doit être obtenu, avant que l'internaute soit rebasculé sur le site initial. Durant ce processus de consentement, l'identifiant universel est partagé entre les différents éditeurs du partenariat. Avec cette configuration, plusieurs obstacles sont franchis simultanément ; tout d'abord, les utilisateurs qui donnent leur consentement l'ont fait d'une manière totalement transparente, les utilisateurs ont un contrôle global sur leurs préférences en matière de vie privée et peuvent les modifier, et pour finir, on assure des informations 1st party plus pertinentes et conformes en tout temps. Sachant que, si un utilisateur retire son consentement en modifiant ses paramètres de confidentialité dans le CMP, son identifiant est supprimé et ne peut plus être utilisé. Une nouvelle obtention du consentement est nécessaire pour recréer un identifiant pour cet utilisateur. Une façon de faire

efficace qui rapproche les acteurs médias et respecte la vie privée des utilisateurs, tout en renforçant la pertinence et assurant la pérennité des activités de publicité digitale.

Le mot de la fin

L'avenir de la publicité digitale basée sur des données et préférences d'utilisation est loin d'être condamné. Les acteurs du marché digital ont déjà repensé leurs manières de fonctionner et apportent des améliorations et des solutions nouvelles dans une constellation où la vie privée des internautes est mise en avant et respectée, ce qui permet de minimiser les craintes liées à l'ère post-cookies tiers.

L'avenir de la publicité digitale basée sur des données de préférence d'utilisation n'est pas condamné.

Par contre, bien que les protagonistes du marché aient résolu les problèmes techniques, l'importance du très convoité user consent s'accroît. Le consentement de l'internaute – qui n'est autre que la condition première et sine qua non dans toutes les solutions techniques existantes – doit être obtenu, disponible et révocable.

Le fameux user consent se profile donc comme le nouvel eldorado, l'or de la prochaine ère digitale, sans cookies. Ce consentement qu'il va falloir obtenir, traiter et manipuler avec soin, sous haute surveillance et suivant les rôles et responsabilités de chaque acteur dans l'écosystème. Une réflexion qui entraine un autre questionnement ; quelles contreparties vont être proposées par les éditeurs principalement pour l'obtention de ce fameux consentement ? La fin des cookies tiers pourrait bien ici signifier une inflation de la valeur de ce consentement, et finalement la nécessité pour les éditeurs et acteurs publicitaires de partager les revenus de la publicité avec les consommateurs.