LES DISPOSITIFS DE MESURE D'AUDIENCE ET DE FRÉQUENTATION DANS LES ZONES ACCESSIBLES AU PUBLIC

Quelles sont les obligations du responsable de ce traitement et comment les respecter ?

Dans une société de plus en plus concurrentielle, la collecte et l'exploitation des données clients sont devenues essentielles au développement de l'activité des entreprises.

Ceci a été parfaitement compris par les entreprises propriétaires de grands espaces privés accessibles au public tels que les **centres commerciaux**, les **grandes surfaces** ou encore les **aéroports** ou **gares** qui font de plus en plus appel à des dispositifs de mesure d'audience et de fréquentation, impliquant la **collecte de données à caractère personnel** telles que l'identifiant d'un téléphone portable (adresse MAC par exemple).

Ces dispositifs offrent de **nombreux avantages** puisqu'ils permettent notamment de mesurer le nombre de personnes dans un magasin à un moment déterminé, de modéliser les trajets réalisés par les clients, d'estimer le temps des files d'attente, de calculer les taux de répétition des visites et, ainsi, d'améliorer les services proposés, voire de louer des espaces plus chers compte tenu du taux de fréquentation ou d'optimiser l'espace afin de mettre en avant certains produits.

Dans la mesure où ces traitements impliquent un **suivi systématique des personnes au moyen d'un dispositif technique**, **le responsable de ce traitement** – qui sera, en fonction de la situation, le propriétaire ou l'exploitant de l'espace – **se doit non seulement de respecter les obligations mises à sa charge par le Règlement général sur la protection des données** (RGPD) mais également d'en **justifier le respect.**

Sommaire :

Quelles sont les obligations à respecter?

QUELLES SONT LES OBLIGATIONS A RESPECTER ?

I. INDIQUER CE TRAITEMENT DANS VOTRE REGISTRE DES ACTIVITÉS DE TRAITEMENT

Toute entreprise traitant des données à caractère personnel sur base d'un dispositif de mesure d'audience et de fréquentation doit, en qualité de responsable de traitement, disposer d'un **registre des activités de traitement** conformément aux dispositions de l'article 30 du RGPD.

Le responsable de traitement devra identifier dans ce registre, outre le **traitement** réalisé, le **type de données** collectées, la **finalité** poursuivie, le **destinataire** des données, la **durée de conservation** des données, les **mesures de sécurité** adoptées ainsi que **la base légale** qui justifie le traitement.

II. DETERMINER LA BASE LEGALE JUSTIFIANT LE TRAITEMENT

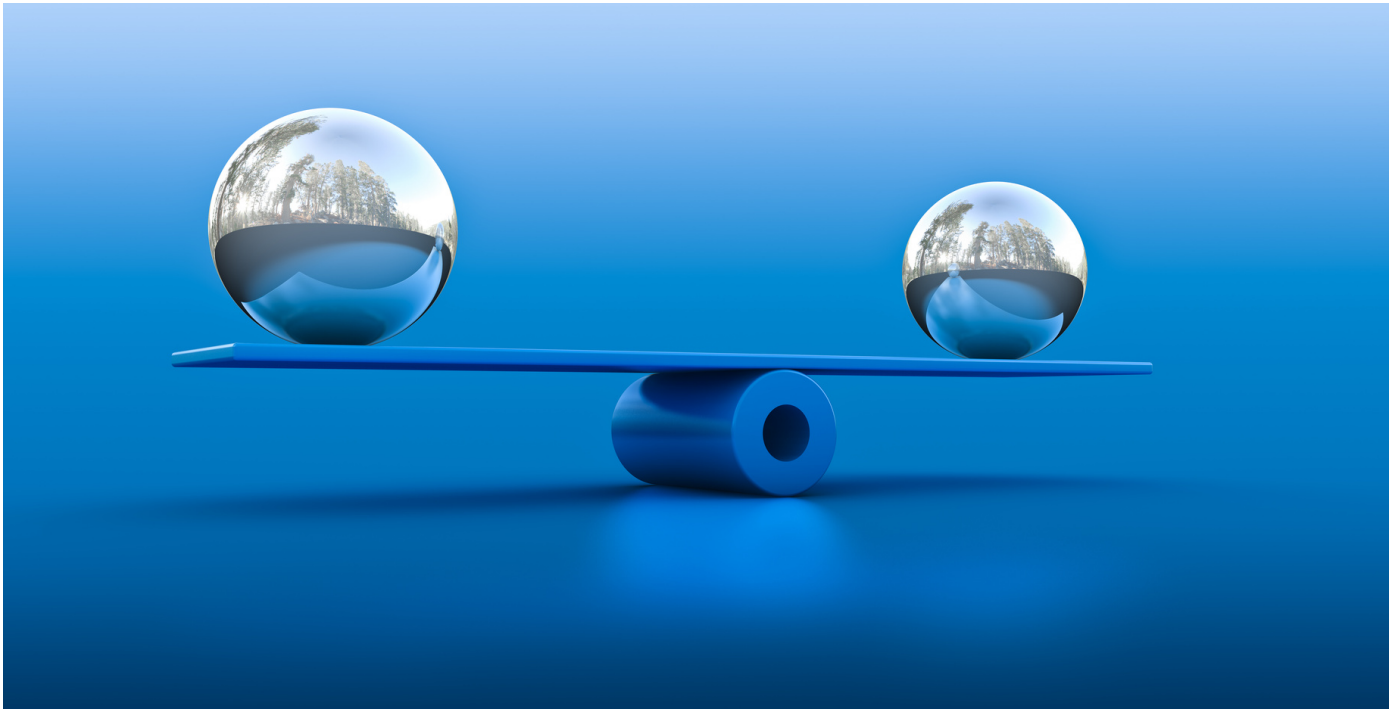
Le principal enjeu pour les entreprises souhaitant recourir à ce type de dispositif est de savoir si la collecte des données des visiteurs peut être fondée:

- sur **l'intérêt légitime (1);**
- ou si elle nécessite d'obtenir **le consentement préalable des personnes concernées (2).**

1) L'INTÉRÊT LÉGITIME POURRA ÊTRE UTILISÉ DANS DEUX CAS :

A. Lorsque les données collectées dans ce cadre sont anonymisées "à bref délai", soit dans les minutes suivant leur collecte

L'entreprise doit cependant s'assurer que **les mesures prises impliquent une réelle anonymisation des données.**



Par « anonymisation » on entend l'utilisation d'un **ensemble de techniques qui rendent impossible, et ce de manière irréversible, l'identification de la personne concernée**.

Aucun lien ne peut donc plus être établi entre les données collectées et la personne concernée. A noter qu'il existe des critères permettant de s'assurer qu'un jeu de données est réellement anonyme.

B. *Lorsque les données sont immédiatement pseudonymisées puis anonymisées ou détruites au bout de 24h.*

La pseudonymisation implique que les données ne puissent plus être attribuées à une personne physique sans une clef d'identification conservée séparément et soumise à des mesures de sécurité techniques et organisationnelles.

Le recours à l'intérêt légitime implique par ailleurs pour le responsable de traitement:

- de pouvoir prouver, par la réalisation d'un triple test, que ses intérêts et les intérêts de la personne concernée ont été mis en balance et que les premiers prévalent **[triple test].** A défaut de cette preuve, le responsable peut se voir imposer une amende.
- de permettre au visiteur d'objecter, à tout moment et simplement (soit sans coût ou formalités administratives excessives), au traitement de ses données [droit d'opposition].

Exemple de technique facilitant ce droit d'opposition : un centre commercial à Rennes a mis en place un système de marquage au sol à l'entrée du centre permettant à la personne qui s'y place d'exercer son droit d'opposition ;

A noter que pour la CNIL, "la désactivation du wi-fi sur le téléphone ou toute technique contraignant les passants à se priver d'une fonctionnalité de leur appareil pour éviter d'être tracé ne peut être considérée comme une modalité satisfaisante d'exercice du droit d'opposition."

2. HORMIS CES DEUX CAS, IL FAUDRA OBTENIR LE CONSENTEMENT DES VISITEURS, PRÉALABLEMENT À LA COLLECTE ET AU TRAITEMENT DE LEURS DONNÉES.

Ce consentement doit être donné de manière éclairée (ce qui implique une information préalable), **libre** (il ne doit donc pas être conditionné), **univoque** (acte positif clair) et **spécifique** (pour le traitement ici visé).

Pour que le consentement soit recueilli de manière valable, il faut que **le visiteur effectue lui-même un acte positif**, comme par exemple entrer ses données personnelles dans un formulaire de collecte.

Exemples de systèmes utilisés pour le consentement :

- *La mise en place d'un système de « badging » NFC par lequel le visiteur active lui-même le NFC de son téléphone qui sera reconnu par une borne ;*
- *La connexion volontaire à un réseau wi-fi spécifique sachant qu'une telle connexion autorise la collecte et l'utilisation de ses données.*

L'inconvénient du consentement est qu'il **peut être retiré à tout moment** par la personne concernée et qu'il faut donc **proposer des solutions techniques** aux visiteurs afin de pouvoir le faire facilement.

La **preuve du consentement doit être conservée** par le responsable de traitement.

En 2019, la CNIL a considéré que l'acceptation des conditions générales n'emporte pas toujours consentement valide puisqu'il n'est pas exprimé par un acte spécifique clair lorsque les cases sont déjà cochées par défaut, en cas de silence ou d'inactivité. En outre, le consentement ne peut être valide si l'obligation d'information n'a pas été correctement accomplie

(Délibération SAN-2019-001 du 21 janvier 2019).

III. INFORMER LES PERSONNES CONCERNEES

Peu importe la base de licéité retenue, **les visiteurs devront toujours être informés de l'existence d'un tel dispositif.**

Comment ?

- **En apposant à proximité du dispositif** (notamment à l'entrée et à la sortie des centres commerciaux, aéroports, grands-magasins, etc) **une mention précisant la finalité du traitement, l'identité du responsable de traitement et l'existence d'un droit d'opposition.**

- **En communiquant (par exemple via un QR code apposé à l'entrée de la zone ciblée) une information plus détaillée sur le site Internet du centre commercial ou sur tout support qui permettra au visiteur** de prendre connaissance des coordonnées précises du responsable de traitement, du DPO, de l'intérêt légitime poursuivi, des finalités, des destinataires des données, de l'existence d'un transfert éventuel de données, de la durée de conservation et de la possibilité d'introduire une réclamation éventuelle auprès de l'autorité de protection des données compétente.

L'information doit être **facile d'accès**.

Elle doit surtout être fournie de manière **claire** (avec un vocabulaire simple), **compréhensible** (pour le public visé) et **concise**.

Il est donc important d'adapter **la politique vie privée reprise sur le site Internet** du Centre commercial notamment. Politique qui est bien souvent négligée et qui doit comporter des dispositions spécifiques.

Exemples de décisions rendues en matière d'information :

- *L'Autorité de protection des données a imposé une amende de 250.000€ à une organisation de groupes publicitaires pour avoir manqué à son devoir d'information puisque « certaines des finalités de traitement sont exprimées de manière trop générique pour que les personnes concernées soient correctement informées de la portée et de la nature exactes du traitement de leurs données à caractère personnel » (Décision au fond 21/2022 du 2 février 2022).*

- *La CNIL, quant à elle, a condamné une société de grande distribution à une amende de 2.250.000€ notamment pour violation du devoir d'information.*

En l'occurrence, elle estimait que « les mentions d'information doivent s'attacher, autant que faire se peut, à utiliser un vocabulaire simple, faire des phrases courtes et employer un style direct, mais aussi éviter les termes juridiques ou techniques, les termes abstraits ou ambigus (…) » et que « malgré le nombre très important d'informations communiquées, ces dernières n'étaient ni hiérarchisées, ni ordonnées. (…) Elle considère qu'une telle présentation ne permet pas aux personnes concernées de trouver facilement l'information qu'elle cherche, la contraignant à lire l'ensemble des mentions d'information. Elle estime donc que la présentation utilisée ne respectait pas l'exigence d'accessibilité posée par l'article 12 du Règlement, éclairée par les lignes directrices sur la transparence déjà citées » (Délibération de la formation restreinte n°SAN-2020-008 du 18 novembre 2020).

IV. REALISER UNE ANALYSE D'IMPACT

La réalisation d'une analyse d'impact permet: **d'identifier et de limiter les risques pour la sécurité et l'intégrité des données** ainsi que **l'impact sur la vie privée des personnes concernées,** notamment en cas de fuite de données, et, d'autre part, **d'évaluer la nécessité et la proportionnalité du traitement.** L'évaluation est donc à la fois juridique et technique.

Cette analyse doit être **réalisée avant la mise en place du traitement** et doit être revue en fonction de son évolution.

Elle doit **obligatoirement** être réalisée chaque fois :

- qu'une évaluation d'aspects personnels suivi d'une décision concernant la personne concernée intervient;
- également, lorsque qu'il existe, comme en l'espèce, une surveillance systématique à grande échelle d'une zone accessible au public (article 35.3.c) du RGPD).

Tel sera le cas également si le traitement utilise des données biométriques pour identifier de façon unique des personnes se trouvant dans un lieu public ou dans un lieu privé accessible au public, si des données sont collectées à grande échelle pour analyser ou prédire la situation économique, la santé, les préférences, centres d'intérêts, la fiabilité, le comportement, la localisation et les déplacements d'une personne soit auprès de tiers, soit au moyen de capteurs, si des données de localisation sont traitées à grande échelle ou de manière systématique et que ce traitement n'est pas strictement nécessaire pour le service demandé, etc.

La réalisation de cette analyse doit être **documentée** en cas de contrôle de l'autorité de protection des données.

V. DEVEZ-VOUS NOMMER UN DATA PROTECTION OFFICER (DPO)?

Le RGPD impose la désignation d'un DPO lorsque les activités de base du responsable de traitement impliquent un **suivi régulier et à grande échelle de personnes concernées.**

Compte tenu du taux de fréquentation des centres commerciaux ou des grandes enseignes, un nombre très important de données est collecté sur les visiteurs dans le cadre de l'analyse d'audience et de fréquentation.

En l'occurrence, bien que le traitement des données ne constitue pas le core-business de l'entreprise, il implique un **suivi à grande échelle**, surtout, lorsque la collecte de données inclut un profilage (pratique dont l'utilisation est strictement règlementée).

Il est dès lors **conseillé de désigner un DPO**, de préférence externe afin d'en assurer la totale indépendance (nous vous invitons, à ce sujet, à consulter notre article "Zoom sur: le délégué à la protection des données - pourquoi, quand et comment choisir un DPO?").

Julie Lodomez
Avocate - Associée
et Cassandra Bockstael
Avocate

Le cabinet LawellMcMiller est à votre disposition pour étudier avec vous les solutions techniques envisageables à l'installation d'un dispositif de tracking conforme au RGPD ainsi que pour la réalisation de toutes les formalités requises par le RGPD telles que l'élaboration d'un registre, d'une politique d'information, etc.

Le présent document a une portée informative, indicative et non contractuelle. Il n'emporte pas un conseil sur un cas particulier.

LawellMcMiller

Bruxelles - Paris
28, Avenue Marnix - 1000 Bruxelles
Belgique
+32 2 736 40 90

https://www.lawellmcm.com/

ALTA-JURIS INTERNATIONAL

Membre du réseau Alta Juris International

https://www.altajuris.com/