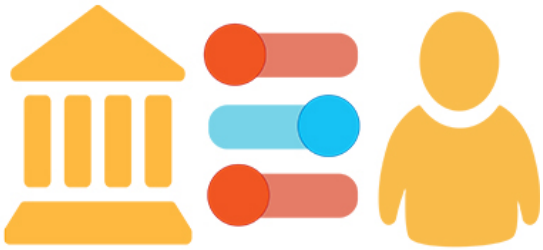
Publié dans MesInfos le 02/11/2017 (dernière mise à jour le 02/11/2017)
Tags : Uncategorized
http://reseau.fing.org/blog/view/169921/retour-sur-mydata-2017-%E2%80%93-consentement-eclaire-all-i%E2%80%99m-askin%E2%80%99-is-for-a-little-respect
Page générée le 15/11/2018 à 18:23

Retour sur MyData 2017 – Consentement éclairé : All I'm askin' / Is for a little respect

La Fing coorganisait pour la seconde année consécutive la conférence MyData2017, qui se tenait du 30 août au 1er septembre dernier, à cheval sur deux villes : Tallinn et Helsinki.

Nous vous proposons de revenir sur quelques-uns des enseignements ou faits marquants de cet événement. Après un premier article d'introduction, centré sur le réseau MyData – son organisation, ses principes (et ses malentendus) puis un second article sur la valeur sociale et sociétale des données (partie I et II), nous avons souhaité nous attarder sur la question du consentement éclairé.

Sujet récurrent du traitement des données personnelles ; à la fois tangible, universel et partie intégrante de l'agenda du GDPR, le consentement avait bien évidemment une place de choix à la conférence MyData 2017. Entre solutions, visions, mais peut-être aussi égarements, ce fut une fois de plus un sujet richement traité. C'est particulièrement troublant de constater comme ce sujet, qui semble isolé et précis, est à la fois une métaphore et la face immergée de l'iceberg de MyData dans son ensemble.



La situation actuelle

On retrouve, sur le sujet du consentement, les adversaires habituels de MyData : « mais cela ruinerait mon business model », « de toute manière, l'utilisateur clique sans regarder … », « je ne sais pas, je ne me suis jamais posé la question »… Les grands gagnants actuels de la collecte et du traitement des données personnelles (GAFAM, régie de publicité en ligne, brokers de données …) ont perfectionné au fil des années leurs techniques pour obtenir ou se passer de consentement. C'est le classique « Lie and Agree » évoqué par Michele Nati désignant la case à cocher en haut des nombreuses pages de CGU. Mais c'est aussi le cas de très nombreux services et applications de startups.

Cette méthode de « non-faire » est devenue un standard, dans un milieu où les GAFAM restent le modèle à suivre. C'est d'ailleurs le constat de Ziad Wakim : alors que le respect des (futurs) utilisateurs, et donc de leur vie privée, fait souvent parti des valeurs principales de la startup aux premiers pas de l'aventure, la gestion respectueuse des données personnelles, et le soin apporté au recueil du consentement sont souvent délaissés, parfois par choix, mais surtout par facilité, conformisme puis négligence.

On le sait, les utilisateurs ne lisent pas ces pages de CGU, ou simples lignes de demande de consentement, qui sont donc seulement des irritants dans le parcours utilisateur. On ne peut que confirmer ce constat, en pensant aux bannières quant à l'usage des cookies qui ont fleuri sur les sites web européens.

Pour compléter le tableau, comme pour le sujet des données personnelles en général, de nombreuses entreprises constatent le grand désordre qui règne au sein de leur système d'information et de leurs produits sur ces questions. À MyData, les témoignages de consultants étaient, sur ce point, concordants (Sami Laine, Sabri Skhiri). Si dans de nombreux cas, les consentements sont rigoureusement recueillis conformément au droit en vigueur ; leur présentation, leur dénombrement, leur consultation ultérieure par le responsable de traitement, comme par la personne concernée sont beaucoup plus difficiles et aléatoires ; sans évoquer les cas de sous-traitance, carrément opaques.

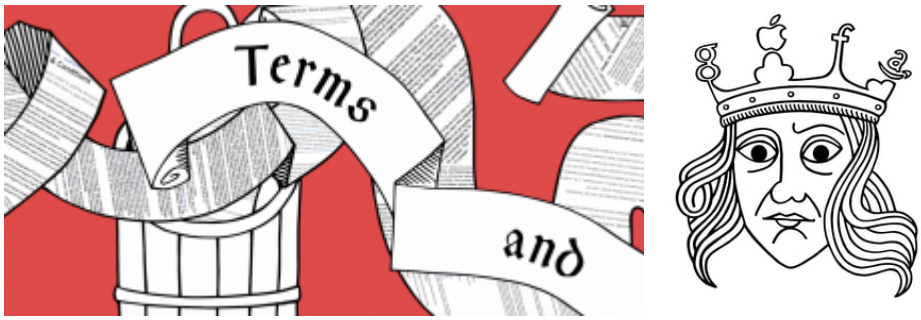
#GDPR
C'est dans ce contexte que va entrer en vigueur (le 25 mai 2018, dans un peu plus de 6 mois) le GDPR, qui est très strict quant au

recueil du consentement, à la conservation et à l'auditabilité des preuves de consentement. Si les lignes n'ont que peu bougé par rapport au droit actuel (en tous cas en France où ces principes sont en vigueur depuis 40 ans !), c'est surtout l'importance des peines encourues qui donne naissance à un sentiment de panique.

Un éventail de solutions techniques pour répondre à cette nouvelle contrainte juridique

Nouvelles contraintes juridiques, nouveau marché ! Entreprises, startup, consultants, chercheurs, groupes de standardisation, projets open source …, tous ont des solutions pour se mettre en conformité, et même tirer parti du GDPR.
La Digital Catapult présentait les avancées sur leur projet de Personal Data Receipt, déjà présenté l'année dernière. Ce dispositif propose de fournir un « reçu » des consentements, et de l'usage qui en a été fait par le responsable de traitement, directement par email à la personne concernée. Un peu plus tard, dans la même session, Joss Langford présentait des standards ouverts et matures, pour faciliter et rationaliser la gestion des données de consentement. On dénombre aussi plusieurs initiatives pour proposer une sémantique autour des CGU et des consentements, afin que puissent émerger des services sur ces données (présentation uniformisée, agents intelligents de négociations de conditions …).

Robert Madge nous rappelait également que pour une entreprise, dans la plupart des cas, il suffisait de supprimer les données personnelles, pour supprimer les charges et risques associés. De l'autre côté, Stuart Lacey et son entreprise proposent leur solution pour mieux gérer les consentements, et ainsi permettre d'améliorer la relation des services avec leurs utilisateurs, charge ensuite à l'utilisateur de mieux capitaliser ses "biens" (oui, il parlait de données personnelles. Nous y reviendrons).



(« King GAFA and the Magical 0-1 Crop » un projet d'un collectif de designer)

Mais de quoi parle-t-on en fait ?

La conférence MyData, c'est heureusement également un temps qui permet de prendre un minimum de recul sur deux types de visions : d'une part, celle de nombreux fournisseurs de services, où le consentement est une simple étape imposée par la réglementation, qui se résout via des dispositifs techniques et d'autre part, la vision des utilisateurs militants, qui voient le consentement comme une arme de défense.

La présentation de Richard Gommer ("Designing for meaningful consent") prenait un peu de hauteur sur le sujet. Déjà, en replaçant le consentement dans le contexte global de la relation entre le service et l'utilisateur (qui est souvent celle entre l'entreprise et son client), dépassant l'écueil où l'on cherche uniquement à comprendre pourquoi l'utilisateur n'a pas cliqué sur la case de consentement, plutôt que de comprendre pourquoi il n'a pas consenti. R.Gommer démystifie l'aspect numérique de ces interactions, en replaçant ces interactions « en ligne », comme faisant partie du monde réel : le *privacy paradoxe* (se dire inquiet de sa vie privée en ligne, mais ne rien faire pour se protéger) n'est alors pas plus paradoxal que la difficulté à arrêter de fumer, ou celle de suivre un régime. Pour lui, le consentement est une interaction avec l'utilisateur, que celui-ci peut voir comme un moment de choix, d'approbation du service : « je donne mon consentement, car je souhaite utiliser le service » ou au contraire « jusque là je n'étais pas très intéressé, ou je n'avais pas bien compris ce que faisait ce service, alors non, je ne suis pas intéressé de poursuivre l'expérience, je ne donne pas mon consentement ». Richard Gommer pousse alors un outil très simple pour changer l'état d'esprit des concepteurs de service : changer les « metrics » qui guident les concepteurs :
1) Thoughtfulness VS speed (la prévenance plutôt que la vitesse),
2) Dropability vs retainment (la propension à l'abandon plutôt que la rétention),
3) Consentfulness VS sign-ups (le consentement plutôt que les inscriptions)

Pour poursuivre sur la démystification, la même session a donné la parole au Dr Frances Burns et à Elizabeth Nelson qui nous exposent leurs recherches sur l'opinion des individus par rapport au traitement de leurs données personnelles, et au consentement. Dans le cadre d'un grand programme d'étude du gouvernement sur la santé des personnes âgées de plus de 50 ans en Irlande du Nord, les chercheurs ont été amenés, comme la loi au Royaume-Uni le leur permet, à croiser ces données médicales avec d'autres données personnelles, détenues par l'État (impôts, domicile, revenus …). Dans un souci de transparence, les deux chercheuses ont réuni quelques personnes

de ce panel (~20) pour leur présenter ce qu'elles souhaitaient faire avec leurs données personnelles, dans quel but, avec quelles mesures de précaution, etc, puis leur ont soumis un questionnaire pour recueillir leur consentement. Les résultats furent quasiment unanimes : "oui vous pouvez réutiliser nos données. Mais pourquoi avez-vous attendu tout ce temps pour le faire !?" Cette expérience montrant que si les personnes ont confiance dans le responsable de traitement (au Royaume-Uni, 90% des individus ont confiance dans l'état, 50% dans les NGOs, et 40% dans les entreprises quant au respect de leurs données personnelles) et si la finalité est comprise et approuvée par les individus, alors ceux-ci sont enclins à accepter l'utilisation de leurs données personnelles.

Ces deux présentations viennent appuyer les constatations que nous avons pu faire au cours du projet MesInfos. Notamment les résultats de recherche de l'expérimentation MesInfos (2014), qui faisaient apparaître que le facteur le plus décisif, était bien celui de la confiance de l'utilisateur dans sa propre maîtrise d'internet : moins ils maîtrisent cet aspect, plus l'étendue de la confiance qu'ils doivent accorder aux services est importante.
Les services n'ont d'autre choix que de construire une relation de confiance pour engager leurs utilisateurs. La confiance c'est se mettre en situation de vulnérabilité, avec optimisme. L'utilisateur se sent déjà en situation de vulnérabilité du fait du manque de maîtrise sur le potentiel et la portée de ses actes sur les dispositifs numériques, or c'est dans cette situation là qu'on lui demande d'accorder sa confiance aux services, en lui demandant de se dévoiler, de fournir un consentement pour permettre au service de s'immiscer dans sa vie privée.

Après un tel tableau, on comprend mieux que le consentement éclairé semble difficile à obtenir. C'est le rôle de ces nouveaux outils (comme ceux cités plus haut) : redonner un peu de pouvoir à l'utilisateur. Mais ce sont bien les services eux-mêmes qui ont le plus d'opportunités de se montrer dignes de confiance. Le coeur de la question reste bien évidemment la finalité : est-ce que le service qui a besoin de ces données personnelles est réellement intéressant ? Par exemple, est-ce que donner l'information des lieux où je suis, l'accès à mes photos, pour permettre l'affichage plus ciblé de publicité, m'intéresse vraiment ? Encore une fois, il ne s'agit pas de négocier sur le prix de vente du droit à l'image de mon chat, mais bien de décider si l'on laisse un inconnu intangible toucher à notre vie privée (comme me le rappelait vivement Christophe Benavent, membre de l'équipe recherche MesInfos, entre deux conférences).

Le GDPR, n'est pas nécessairement une grande avancée pour les droits des individus, c'est surtout un constat de l'absence de respect qui est peu à peu devenu la norme des relations entre services numériques et usagers ; mais souvent aussi entre les entreprises et leurs clients grand public. Tout dépendra de ce que les acteurs (entreprises, acteurs publics, startups, concepteurs de services…) en feront. Espérons qu'il aidera ou sera le contemporain d'améliorations qui permettront réellement de faire progresser le sujet de la confiance, et donc du consentement "éclairé" et ne rajoutera pas seulement de nouvelles clauses dans les CGU et de nouvelles bannières sur les sites…

Article importé: http://mesinfos.fing.org/retour-sur-mydata-2017-consentement-eclaire-all-im-askin-is-for-a-little-respect/
Par: Guillaume Jacquart
Publié: November 2, 2017, 12:37 pm