Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CONSEIL GÉNÉRAL DE L'ÉCONOMIE
DE L'INDUSTRIE, DE L'ÉNERGIE ET DES TECHNOLOGIES

TELEDOC 792
BATIMENT NECKER
120, RUE DE BERCY
75572 PARIS CEDEX 12

N° 2017/17/CGE/SG

Janvier 2018

Accès aux données, consentement, l'impact du projet de règlement e-privacy

Rapport à

Monsieur le ministre de l'Économie et des Finances

Madame la ministre de la Culture

Monsieur le secrétaire d'Etat chargé du Numérique

établi par

Claudine DUCHESNE - JEANNENEY
Contrôleur général économique et financier

Gérard LALLEMENT
Ingénieur général des mines

Jacques SERRIS
Ingénieur général des mines

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

SOMMAIRE

SYNTHESE

Le ministre de l'Economie et des Finances, la ministre de la Culture et le secrétaire d'Etat auprès du Premier ministre chargé du numérique ont chargé le Conseil général de l'économie d'une mission sur l'impact des mesures de protection des informations stockées dans les équipements terminaux de communication électronique, prévues par le projet de règlement e-privacy (articles 8, 9 et 10). Ce projet est présenté comme une lex specialis du Règlement général sur la protection des données personnelles (RGPD), qui entrera en vigueur en mai 2018.

A l'issue de nos analyses, nous pensons que le RGPD et le projet de règlement e-privacy répondent à une véritable attente, d'amélioration de l'information et de la protection de la vie privée des internautes. Mais, tel qu'il est proposé, le projet de règlement e-privacy, au-delà du RGPD, risque de renforcer la position des grandes plateformes du Net qui disposent d'utilisateurs réguliers, dont une large part a ouvert un compte. Parallèlement, il risque d'affaiblir les acteurs exploitant des services ou sites qui servent des clients occasionnels. S'il impose un paramétrage des logiciels d'accès aux services de communication électronique selon des modalités dont l'ergonomie n'a pas été testée et dont on ne sait pas s'il répond au besoin des utilisateurs, il pourrait susciter une réaction de rejet parmi ceux-ci.

Ce constat s'appuie sur l'étude des usages des services de communication électronique. Le temps passé sur Internet rattrape le temps passé à la télévision, et assez logiquement, les recettes publicitaires numériques ont dépassé depuis 2016, celles de la télévision. Le succès de la publicité numérique vient du développement de la publicité comportementale, qui a permis aux annonceurs de basculer du média planning à l'audience planning, c'est-à-dire à des campagnes conçues selon le profil des individus auxquels on va envoyer le message. Ces techniques valorisent les espaces publicitaires, ce qui est particulièrement important pour les sites généralistes, qui ne peuvent pas proposer de la publicité contextuelle. Sans données, la publicité est moins efficace et la valeur des espaces publicitaires baisse. Mais, bien sûr, le recueil des données personnelles exige le consentement de l'internaute.

Les internautes continuent à apprécier le modèle du tout gratuit, financé par la publicité. Bien qu'ils accordent beaucoup de valeur à leurs données personnelles, deux tiers d'entre eux sont disposés à partager des données pour accéder à des contenus ou à des services et plus de huit sur dix préféreraient accéder à des sites gratuits avec publicité plutôt que de payer pour des contenus. Ce paradoxe entre une volonté de se protéger et l'acceptation du partage des données n'est qu'apparent. Ce qu'une grande part des internautes refuse, ce n'est pas la publicité ou la constitution de bases rassemblant leurs données mais le fait de ne pas être informés de la collecte et des usages de ces données.

Le projet de règlement donne une position privilégiée aux logiciels d'accès aux services de communication électronique. Dans la plupart des cas (navigateurs, systèmes d'exploitation, assistants personnels …) les éditeurs de ces logiciels sont peu nombreux et certains occupent une position dominante sur leur marché. Ils vont se trouver dans une situation particulière : ils devront recueillir le consentement des internautes pour les données qu'ils utilisent pour leurs besoins propres, alors qu'ils apparaitront comme les garants de la protection de la vie privée de ces mêmes

internautes, vis-à-vis des services tiers. Ils seront dans une position privilégiée pour assurer un dialogue avec l'internaute, lui fournir des explications et in fine, recueillir son consentement.

D'autres grandes plateformes du net, comme les réseaux sociaux et les très grands sites de e-commerce, qui disposent d'utilisateurs réguliers ayant généralement ouvert un compte, seront également bien placées dans le dialogue avec les internautes pour leur expliquer leur politique de respect de la vie privée. En revanche, les autres fournisseurs de services qui dépendent d'une clientèle plus occasionnelle auront plus de difficultés.

Nous proposons quatre principes qui pourraient guider la réflexion et inspirer les positions françaises lors de la poursuite de la négociation du texte du règlement :

- **Pour préserver la vie privée de façon durable, le règlement doit être neutre technologiquement.** La variété des marchés (services de communication électroniques fixes, mobiles, internet des objets - des montres aux véhicules connectés) et pour chaque marché, la variété des options (paramétrage ou options des logiciels d'accès, installation d'extensions comme un logiciel de protection contre le tracking, un ad-block ou un anti-virus), montrent l'impossibilité de définir des spécifications techniques qui couvriraient un champ aussi large.

- **L'offre de logiciels permettant la protection de la vie privée doit continuer à se diversifier et à s'enrichir.** Cette offre peut relever d'une fonction proposée par l'éditeur d'un logiciel d'accès ou d'une extension, qui peut être fournie par une autre société. Il faut que ces divers logiciels d'accès ou de contrôle d'accès soient considérées au même niveau, sans donner un rôle de gardien à certains d'entre eux. En dehors des questions liées à la protection de la vie privée, les autorités chargées du respect du droit de la concurrence doivent examiner l'incidence des options proposées par les logiciels d'accès à des services de communication dont les éditeurs occupent une position dominante sur leur marché.

- **Pour préserver un Internet ouvert, il faut offrir une « voie de retour ».** Les services ou sites qui servent des utilisateurs occasionnels ont besoin de créer un contact direct avec eux, pour leur permettre de personnaliser leur offre, ou de présenter les options économiques de la fourniture du service. Une entreprise doit avoir l'opportunité de conditionner l'accès à ses services à l'acceptation de différentes conditions (abonnement, publicités …). Ce dialogue avec l'internaute pour le solliciter, recueillir son consentement et le cas échéant, modifier, pour le site considéré, le paramétrage du logiciel de contrôle qui a permis l'accès au service considéré constitue une « voie de retour ». Les délais de mise en œuvre du règlement e-privacy doivent être aménagés pour que ces options trouvent une concrétisation technique.

- **Il faut réguler la pression publicitaire sur Internet.** La montée des Ad-block traduit une dégradation de l'expérience utilisateur. Pour autant, la régulation de la pression publicitaire ne relève pas au premier chef du règlement e-privacy. C'est d'abord aux professionnels de la faire par autorégulation. Une meilleure image de la publicité auprès des internautes serait de nature à faciliter le recueil de leur consentement pour des publicités ciblées.

Ce rapport répond à une commande du gouvernement auprès du CGE. Ses analyses et propositions reflètent les conclusions des rapporteurs et n'engagent pas la position du gouvernement vis-à-vis du projet de règlement e-privacy.

TABLE DES RECOMMANDATIONS

INTRODUCTION

Par lettre de mission du 23 octobre 2017, le ministre de l'économie et des finances, la ministre de la culture et le secrétaire d'Etat auprès du Premier ministre chargé du numérique ont chargé le vice-président du conseil général de l'économie de mener une mission relative aux articles 8, 9 et 10[1] de la proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques (ci-après, dans ce document, « le projet de règlement e-privacy »). Il est demandé à la mission de « *fournir des éléments d'analyse qui permettraient d'apprécier plus précisément l'impact des mesures envisagées dans le projet de règlement sur les acteurs concernés à la fois sur le plan économique (manque à gagner, investissement pour se maintenir ou s'adapter …) et sur le plan technologique, à travers la description des solutions d'adaptation qui pourraient être mises en œuvre, en tenant compte de leur acceptabilité sociale (caractère intrusif ou répétitif) et de leur ergonomie (facilité d'usage)* ».

Après un bref rappel sur la portée du règlement e-privacy, la mission s'est attachée à :

- analyser les nouveaux usages des services de communication électronique au regard du respect de la vie privée, en illustrant cette démarche par quatre études de cas – les navigateurs internet, les applications mobiles, les assistants numériques et le véhicule connecté ;
- étudier l'approche réglementaire des Etats-Unis et la démarche d'Apple en matière de e-privacy ;
- décrire différentes options techniques mises en œuvre pour paramétrer la protection de la vie privée (logiciels d'accès ou extensions logicielles) ;
- étudier les impacts de la mise en œuvre du projet de règlement sur les acteurs économiques.

Sur la base de ces constats et analyses, la mission a élaboré des recommandations articulées autour du respect de la vie privée et de la préservation des intérêts des acteurs économiques. Ce rapport répond à une commande du gouvernement auprès du CGE. Ses analyses et propositions reflètent les conclusions des rapporteurs et n'engagent pas la position du gouvernement vis-à-vis du projet de règlement e-privacy.

1 E-PRIVACY, UN REGLEMENT AUX INTENTIONS CLAIRES MAIS A LA PORTEE ENCORE INCERTAINE

1.1 Le règlement et ses articles 8, 9 et 10

La Commission européenne a présenté le 10 janvier 2017 une proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques (ci-après « le règlement *e-privacy* »), présenté comme *une lex specialis* du Règlement général sur la protection des données personnelles (RGPD) adopté en avril 2016 et entrant en vigueur le 25 mai 2018.

[1] Voir annexe 4

La proposition de règlement e-privacy trouve son fondement dans les articles 16 et 114 du traité sur le fonctionnement de l'Union européenne (TFUE). Aux termes du premièrement de l'article 16 du TFUE « *toute personne a droit à la protection des données à caractère personnel la concernant* ». Les communications électroniques faisant intervenir des personnes physiques et devant être considérées à ce titre comme comportant des données à caractère personnel, la protection des personnes physiques à l'égard de la confidentialité des communications et du traitement de ces données se fonde sur l'article 16 du TFUE.

La proposition se fonde également sur l'article 7 de la Charte des droits fondamentaux : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* », de même portée que l'article 8, paragraphe 1, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH): « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ».

En application de la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme, les activités professionnelles des personnes physiques sont incluses dans le champ du droit garanti par l'article 7 de la Charte des droits fondamentaux et par l'article 8 de la CEDH.

Le règlement e-privacy proposé fait suite aux dispositions des directives 97/66/CE, 2020/58/CE et 2009/136/CE. La directive 2009/136/CE renforce le consentement préalable de la personne concernée pour le stockage d'informations ou pour l'accès à des informations dans l'équipement terminal de l'utilisateur.

La proposition de règlement e-privacy fait partie du 2ème pilier « *mettre en place un environnement propice au développement des réseaux et services numériques* » de la « stratégie pour un marché numérique unique en Europe » présentée par la Commission européenne le 6 mai 2015.

En décembre 2017, il existe 2 versions du projet de règlement : la version initiale proposée par la Commission en janvier 2017 et une version votée par le Parlement européen en octobre 2017 (voir annexe 4).

1.2 Quelle sera l'extension juridique du projet de règlement e-privacy ?

Un des objets du projet de règlement est d'étendre les règles de protection de la vie privée à des nouveaux services de communications interpersonnelles sur Internet (voix sur IP, messagerie instantanée, mail …) qui ne sont pas soumis au cadre réglementaire actuel de l'Union en matière de communications électroniques, notamment à la directive « vie privée et communications électroniques ». Sont également concernées les entreprises qui fournissent des services utilisant ou rendant possible une communication électronique, même en tant que fonction mineure accessoire au service rendu. Enfin la proposition de règlement devrait s'appliquer à l'établissement des communications de machine à machine.

La question de la protection de la confidentialité des communications électroniques et des équipements terminaux n'est pas abordée par le RGPD, qui ne définit pas quels fondements juridiques peuvent être permis pour le traitement et dans quelles situations, dans la mesure où il fixe le cadre général de la protection des données à caractère personnel. L'actuelle directive 2002/58/CE encadre déjà ce type d'activité, la proposition de règlement e-privacy précise ces points.

Le règlement fonde la protection des « utilisateurs finaux » sur le consentement. La définition de l'utilisateur final couvre les personnes physiques et les personnes morales. Les communications de

machine à machine sont également couvertes. Mais le cas d'une chaîne d'approvisionnement, qui relève des relations inter-entreprises, est très différent de celui d'une montre connectée. Pour les personnes morales comme pour les objets connectés, il faudra préciser le mode de recueil du consentement.

L'analyse juridique du projet de règlement dépasse le cadre de la mission. Cependant, tous les interlocuteurs reçus par la mission ont souhaité souligner la complexité du sujet et nous ont fait part de leurs interrogations. Les points suivants sont revenus systématiquement lors des entretiens menés par la mission et méritent d'être signalés :

- l'intérêt économique du fournisseur de service n'est pas pris en considération dans le champ des exceptions au consentement prévu dans e-privacy, à l'inverse du RGPD ;
- concernant l'interprétation de la notion de « tracking wall », les éditeurs à la recherche de leur équilibre économique soulignent la nécessité de pouvoir proposer différents formats, en fonction de la décision de l'internaute d'accepter ou non les publicités ciblées ;
- de nombreux juristes estiment que le paramétrage d'un logiciel d'accès, prévu dans e-privacy, ne pourra pas exonérer un fournisseur de service du recueil du consentement spécifique au titre du RGPD ;
- il est impossible d'estimer les coûts de mise en conformité pour le règlement e-privacy, au moment où les entreprises se préparent à l'entrée en vigueur du RGPD, mais tous expriment la certitude que ce sont les PME qui auront le plus de difficultés.

2 LA VIE PRIVEE A L'EPREUVE DES NOUVEAUX USAGES DES SERVICES DE COMMUNICATION ELECTRONIQUE

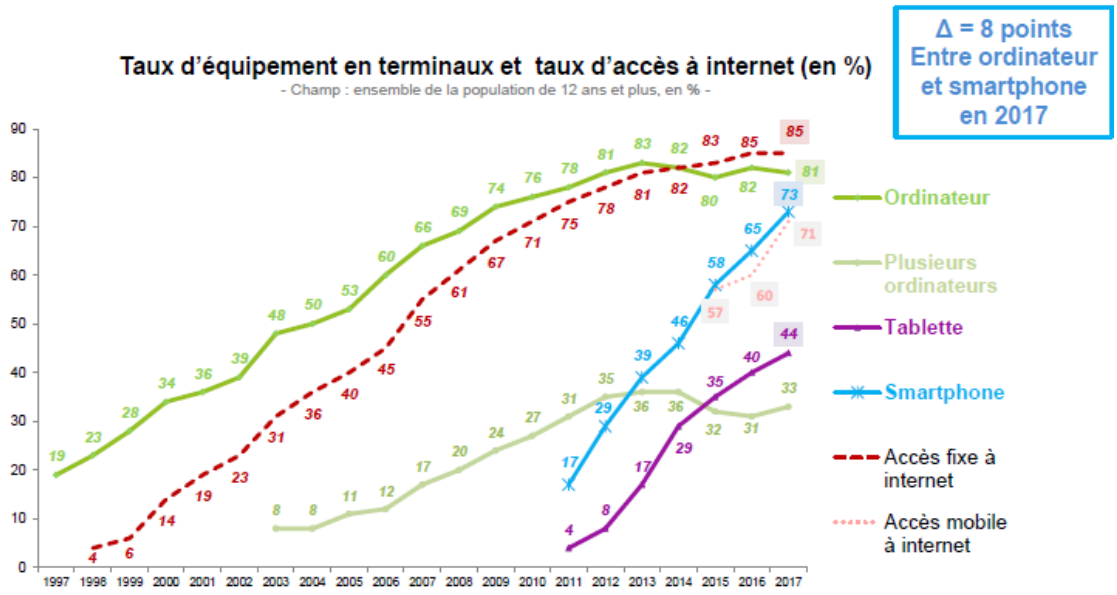
2.1 Les nouveaux usages sont portés par les smartphones et leurs applications

La diffusion des objets communicants s'est fortement accrue depuis les années 2010. Ils constituent autant de **portes d'entrée aux messages transmis sur internet, qu'ils soient de nature publicitaire ou d'information, ciblés ou d'intention générale**.

Quelques chiffres et tendances tirés de l'enquête « Baromètre du numérique[2] » de 2017 méritent d'être signalés :

- plus de neuf personnes sur dix possèdent un téléphone mobile ;
- si l'équipement en ordinateurs tend à stagner, la croissance en nombre d'équipements nomades – tablettes tactiles et smartphones – est particulièrement soutenue depuis le début des années 2010. Près de trois personnes sur quatre sont dotées d'un smartphone et plus de quatre personnes sur dix disposent d'une tablette. Entre 2012 et 2017, le nombre de smartphones a été multiplié par 2,2 et celui des tablettes par 5,5 ;
- le multi-équipement est également une réalité : plus de trois personnes sur dix sont équipées d'un ordinateur, d'une tablette et d'un smartphone.

[2] Source : enquête réalisée par le CREDOC pour le Conseil général de l'économie, l'Agence de régulation des communications électroniques et des postes et l'Agence du numérique relative à la diffusion et à l'usage des technologies de l'information dans la société française. Enquête réalisée au moyen d'entretiens en face à face auprès d'un échantillon représentatif de 2200 personnes de plus de douze ans.

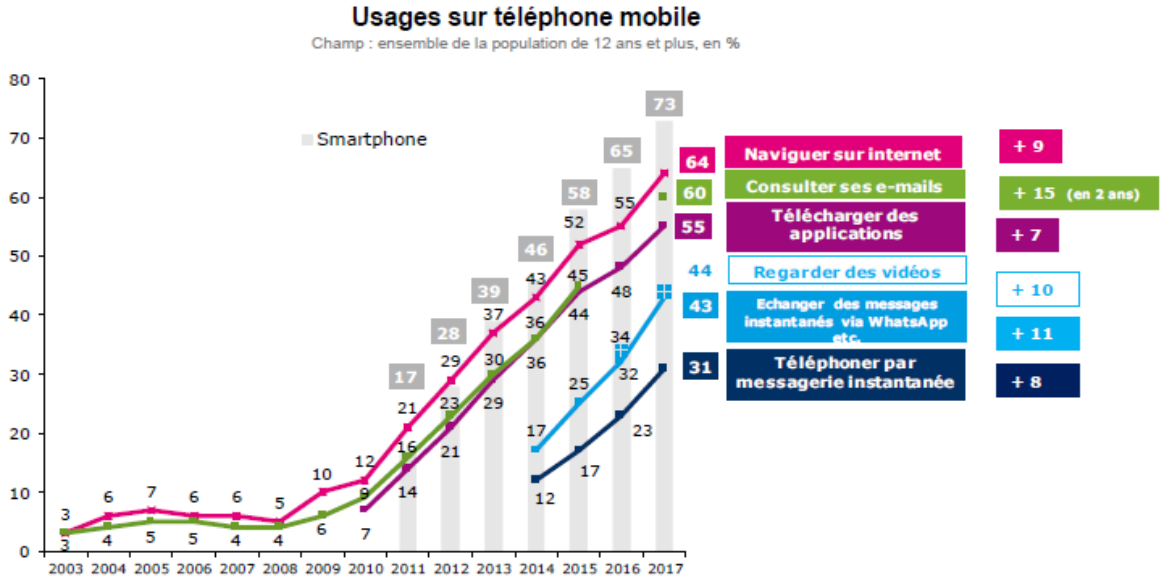


Source : Baromètre du Numérique 2017

Aux objets communicants classiques sont venus s'ajouter depuis peu des outils plus spécifiques comme les intermédiaires transactionnels (Cortana, Siri, Amazon) et de façon plus générale, les objets de l'internet of Things.

La **navigation sur internet, la consultation des emails et le téléchargement d'applications** sont les applications les plus utilisées avec des équipements nomades (respectivement par 64%, 60% et 55% des personnes). L'édition 2016 de l'enquête[3] montrait que **les services de géolocalisation étaient utilisés par 42% des personnes** (la question n'a pas été posée pour l'édition 2017).

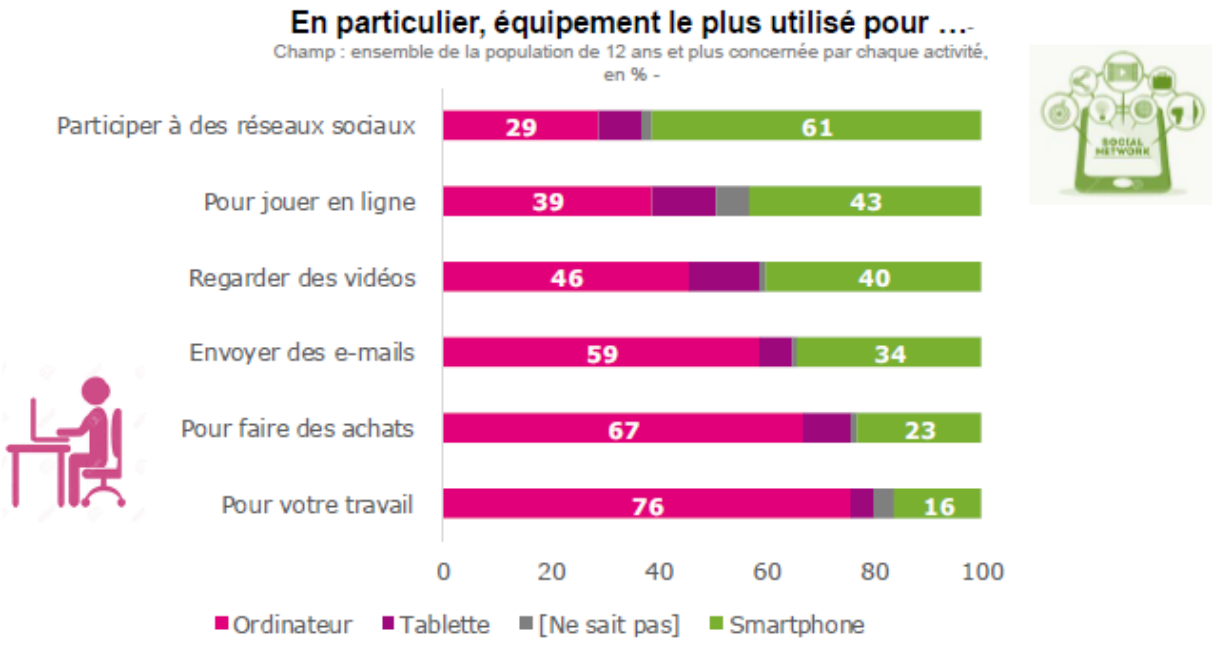
Les **applications fournies par des OTT** (Whatsapp, Hangouts, etc.) connaissent également une forte croissance : 43% des personnes les utilisent pour échanger des messages texte et 31% pour téléphoner.



Source : Baromètre du Numérique 2017

[3] Enquête « Baromètre du numérique » réalisée par le CREDOC pour l'Autorité de régulation des communications électroniques et des postes, le Conseil général de l'économie et l'Agence du numérique

A chaque équipement correspond un usage privilégié : la participation à des réseaux sociaux et le jeu en ligne concernent une majorité d'utilisateurs de smartphones ou de tablettes ; inversement, l'envoi d'emails et les achats en ligne sont réalisés en premier lieu avec des ordinateurs. La visualisation de vidéos se répartit à égalité entre les deux canaux.



On notera aussi que des évolutions importantes concernant en premier lieu les médias sont en cours ou sont advenues. Ainsi le temps passé sur internet est sur le point de rattraper le temps passé devant la télévision (respectivement 18 heures et 20 heures par semaine[4]) et pour la première fois en 2017, deux internautes sur trois sont membres d'au moins un réseau social (86% des internautes de 12 à 40 ans). Elles attestent de la **montée en puissance des univers applicatifs spécifiques (Facebook, Chaînes Youtube, etc.) et par conséquent de leur capacité à drainer un flux publicitaire important et à imposer un format de message spécifique**.

En matière **d'achats sur internet, les caractéristiques de la population** constituent **le déterminant majeur. L**es jeunes adultes (18-25 ans) et les tranches d'âge intermédiaires (25-39 ans) achètent massivement sur internet ; ensemble, ils représentent 84% des acheteurs. La propension à acheter en ligne est **également plus forte chez les plus diplômés, les classes moyennes supérieures et les personnes disposant de hauts revenus**. L'autre **élément à prendre en considération est le niveau de confiance que les sites inspirent**. Plus cette confiance est forte, et plus l'acte d'achat a lieu : 95% des internautes qui ont très confiance dans un site font des achats mais seuls 10% de ceux qui n'ont pas confiance achètent[5].

2.2 Protection de la vie privée : des internautes vigilants et proactifs

En matière de confidentialité et de protection des données personnelles[6], 54% des internautes se déclarent plus vigilants sur internet que les années précédentes. Surtout, les internautes estiment

[4] Edition 2016 du baromètre du numérique.

[5] Edition 2016 de l'enquête « Baromètre du numérique ». La question n'a pas été posée en 2017.

[6] Synthèse du rapport « Données personnelles et confiance : quelle stratégie pour les citoyens-consommateurs en 2017 ? », Chaire Valeurs et Politiques des Informations Personnelles, Patrick Waelbroeck, Armen Khatchatourov, Claire Levallois-Barth, 23 juin 2017.

que les données partagées doivent être spécifiques à l'usage qu'ils en attendent : ainsi, ils communiquent les informations liées à leur identité aux services de l'Etat ou à leur banque (54% des internautes communiquent la copie d'une pièce d'identité, 43% leurs coordonnées bancaires et 31% des informations relatives à leur santé) mais ils les refusent aux réseaux sociaux. 40% des internautes ne souhaitent pas partager leurs données sur les réseaux sociaux et 10%, s'ils avaient le choix, souhaiteraient ne fournir aucune information à aucun acteur.

On assiste en parallèle à l'établissement de comportements de défiance : 61% des internautes refusent de partager leur géolocalisation, 59% effacent leurs traces de navigation et 45% configurent les paramètres de protection de la vie privée de leur navigateur. Un internaute sur cinq environ met en œuvre des solutions extrêmes pour se protéger : navigation privée ou anonyme (via le réseau Tor). Dans tous les cas, l'objectif recherché est de limiter le nombre d'informations collectées.

Pour autant, **les personnes qui utilisent des outils de protection sont aussi celles qui consomment le plus** : 52% d'entre elles font un achat en ligne au moins une fois par mois. Avoir les moyens de se protéger donne le sentiment de pouvoir agir sur un environnement ressenti comme intrusif mais les internautes souhaiteraient que les acteurs de l'Internet s'engagent à être plus transparents et à respecter davantage leur vie privée. Ces résultats ne sont pas nouveaux. Ils corroborent ceux de l'enquête de l'enquête « Baromètre du numérique » de 2014[7] qui **montraient que le fait que les données ne soient pas suffisamment protégées constitue, pour 33% des personnes, un frein majeur à l'utilisation d'internet**.

Les internautes sont conscients de risques. En 2014, 86 % des personnes estimaient que des **logiciels peuvent transmettre des informations présentes sur les téléphones** mobiles (comme le carnet d'adresse et la localisation) sans que l'usager en soit averti. Près d'une personne sur deux pensait également avoir déjà été victime d'un accès indésirable à ses données personnelles.

Face à ces risques, les **personnes se disaient majoritairement attentives à la protection de leurs données personnelles**, par exemple en installant un pare-feu ou un logiciel de sécurité, en recourant à des mots de passe ou en stockant leurs données en dehors de toute connexion à internet ; 57 % disaient être très vigilantes et 16 % y pensaient « de temps en temps ».

Ces résultats sont cohérents avec ceux de **l'enquête Eurobaromètre**[8] relative à la vie privée et aux communications électroniques, citée par le projet de règlement e-Privacy, à propos des exigences des personnes vis-à-vis de l'accès à leurs équipements.

2.3 Les internautes cherchent à réduire la pression publicitaire pour améliorer leur confort de navigation

Les bloqueurs de publicité (Adblocks) sont des extensions logicielles des navigateurs dont le but est de filtrer la publicité. Ils permettent un affichage plus rapide et plus clair des pages web, une moindre consommation de ressources (processeur, mémoire vive et bande passante) ainsi qu'une certaine protection de la vie privée par désactivation des systèmes de suivi, de trace numérique, et d'analyse mises en œuvre par les régies publicitaires.

---

[7] Enquête « Baromètre du Numérique » de 2014. Un chapitre de cette enquête est consacré à la confidentialité et à la vie privée.

[8] Enquête Eurobaromètre 443 de 2016 sur la vie privée et les communications électroniques (SMART 2016/079).

Les internautes qui utilisent un Adblock cherchent d'abord réduire la pression publicitaire pour améliorer leur confort de navigation. **Parmi les 55% d'internautes**[9] **qui ont déjà utilisé un bloqueur de publicité, 84% les apprécient pour leur capacité à ne pas afficher les publicités intrusives**. Pour plus d'un internaute sur deux, ils servent à **améliorer le confort de navigation** et pour 36%[10], à **protéger** leurs informations personnelles.

> **Il faut séparer la perception, par les internautes, de la pression publicitaire, qui résulte du format des annonces et de leur volume sur une même page, de leur perception du traçage, liée au respect de la vie privée.**

Si les bloqueurs de publicité sont surtout utilisés sur les postes fixes, les mobiles sont également concernés : une étude[11] de 2016 montre que 309 millions de personnes (16% des 1,9 milliards d'utilisateurs de smartphones dans le monde, ce pourcentage a doublé entre 2015 et 2016) utilisent un bloqueur de publicités sur leur navigateur internet dont 116 millions en Chine, 89 millions en Inde et 28 millions en Indonésie. L'Europe et l'Amérique du Nord seraient moins touchées avec 8,9 millions d'utilisateurs actifs par mois.

Cette montée des adblocks a fait réagir les professionnels de la publicité, qui ont pris conscience des effets négatifs d'une pression publicitaire jugée excessive par les utilisateurs. En 2015, des représentants des groupes de consommateurs (Centre pour la Démocratie et la Technologie, Open Rights Group), des annonceurs (Fédération Mondiale des Annonceurs), des médias (l'Association Mondiale des Journaux, l'Association Nationale des Journaux, la Fédération Internationale des Éditeurs de périodiques), des agences (Havas), des éditeurs de navigateurs (Mozilla, Google), ainsi que de la Commission Européenne, de l'administration britannique et du World Economic Forum se sont réunis dans le cadre de tables rondes sur les bloqueurs de publicité.

Une opinion majoritaire a émergé de ces tables rondes. Les points suivants constituent l'expression des parties prenantes :

- le temps de chargement d'une page doit rester sous un seuil admissible ;
- le nombre d'expositions doit être réduit en ciblant les espaces premium. Cela aura un meilleur impact sur les marques, améliorera l'expérience utilisateur et stimulera la créativité ;
- la qualité des publicités doit être améliorée ;
- la publicité contextuelle doit être préférée au ciblage individuel lorsque l'internaute refuse d'être suivi ;
- les éditeurs doivent inciter leurs utilisateurs à partager leurs données dans le cadre d'une démarche volontaire clairement expliquée ;
- les éditeurs doivent inciter les annonceurs à cibler la valeur plutôt que le prix d'un emplacement ;
- l'utilisateur doit disposer des moyens de refuser et de se plaindre de la publicité qu'il reçoit.

---

[9] Source : rapport « Données personnelles et confiance : quelle stratégie pour les citoyens-consommateurs en 2017 ? », Chaire Valeurs et Politiques des Informations Personnelles, Patrick Waelbroeck, Armen Khatchatourov, Claire Levallois-Barth, 23 juin 2017.

[10] Les ratios d'un internaute sur deux et de 36% des internautes sont rapportés au nombre d'internautes qui installent des bloqueurs de publicité sur leur navigateur (55% de l'ensemble des internautes). Source : Baromètre du numérique 2016

[11] 2016 Mobile Adblocking Report, Pagefair, https://pagefair.com/blog/2016/mobile-adblocking-report

En France, d'autres approches sont en cours, visant à diminuer la pression publicitaire et à effectuer un ciblage plus pertinent des utilisateurs. Les professionnels de la publicité[12] se sont engagés dans une démarche articulée autour de trois axes :

- améliorer l'expérience utilisateur et la qualité des environnements de diffusion (promotion des labels Digital Ad Trust et Coalition for better ads) ;
- améliorer la qualité de la mesure et de la sécurité en imposant des mesures tierces indépendantes fondées sur une méthodologie éprouvée ;
- renforcer l'indépendance des professionnels vis-à-vis des GAFA en matière de données. Celles-ci, nécessaires à la réalisation d'un ciblage pertinent, sont mutualisées au sein de plates-formes regroupant les principales entreprises de médias (Gravity et Skyline).

La montée des ad-block, si elle devait se poursuivre, constituerait une menace économique pour les acteurs de la publicité. Il ne faut pas la confondre avec les enjeux économiques liés à la mise en œuvre du projet de règlement. **La mission considère qu'une autorégulation plus efficace est la bonne réponse à la montée des ad-blocks.**

2.4 Accepter la publicité ou payer : les nouveaux usages restent confrontés à ce dilemme

Depuis les débuts de l'internet, la question se pose : les internautes sont-ils disposés à payer pour accéder à des contenus ou à des services ? Si le New York Times, avec 1,8 million d'abonnés payants purement « numériques » (contre un million d'abonnés à la version papier) a montré sa capacité à mener la transformation numérique de ses éditions, la plupart des organes de presse n'y sont pas encore parvenus. En France, à l'exception des Echos dont la diffusion est pour moitié numérique, **l'édition numérique reste encore un modèle marginal en termes de revenus,** malgré un taux de croissance élevé (+30% en 2017 pour les quotidiens nationaux). La raison principale réside dans **l'appétence des internautes pour le modèle du tout gratuit,** par ailleurs largement financé par la publicité.

Selon une étude de l'*Internet Advisory Board*[13], « *l'expérience en ligne européenne est essentiellement gratuite et financée par la publicité, les deux tiers des utilisateurs ne payant jamais pour les services ou les contenus* ». Selon l'IAB, neuf utilisateurs en ligne sur dix cesseraient d'utiliser les services d'un site s'ils devenaient payants. Les **personnes à « faibles revenus »**[14] **seraient les premières à renoncer** à ces services: 5% d'entre elles seulement seraient disposés à payer contre 12% pour les « hauts revenus »[15]. Bien que les internautes européens accordent beaucoup de valeur à leurs données personnelles, **deux tiers d'entre eux seraient disposés à partager des données pour accéder à des contenus ou à des services**[16] et plus de huit sur dix préféreraient accéder à des sites gratuits avec publicité plutôt que de payer pour des contenus.

Le paradoxe entre une volonté de se protéger et l'acceptation du partage des données n'est qu'apparent. Ce que les internautes refusent, ce n'est pas la publicité ou la constitution de bases de

---

[12] Syndicat des Régies Internet (SRI), l'Union des Entreprises de Conseil et Achat Média (UDECAM)

[13] Europe on line: an experience driven by advertising, Internet Advisory Board, 2017.

[14] Personnes dont les revenus sont dans les trois premiers déciles.

[15] Personnes dont les revenus sont dans les trois derniers déciles.

[16] Chiffre corroboré par l'étude « Données personnelles et confiance : quelle stratégie pour les citoyens-consommateurs en 2017 ? » cf. note précédente

données dont ils sont la matière première mais le fait de ne pas être informés de la collecte et des usages de ces données. Selon l'étude de l'Internet Advisory Board, ils préféreraient obtenir des informations détaillées sur la façon dont leurs données sont utilisées, y compris les raisons pour lesquelles ils voient une annonce particulière, savoir qui peut y accéder et être en capacité de moduler ou d'arrêter leur utilisation, plutôt que de se voir présenter de multiples bannières d'acceptation de cookies (67% vs. 50%).

3 QUATRE ETUDES DE CAS

Alors que le spectre des services de communication électronique couverts par le projet de règlement e-privacy est extrêmement vaste, l'attention portée aux articles 8, 9 et 10 s'est focalisée sur une fonctionnalité déjà ancienne des navigateurs (distinction entre cookies first et tiers). Pour éviter cet écueil et étendre notre démarche, nous passons brièvement en revue les navigateurs internet, les applications mobiles (les Apps), les interfaces conversationnelles et le véhicule connecté. Cette revue nous permet de souligner la diversité des questions soulevées et des solutions proposées pour renforcer la protection de la vie privée.

3.1 Les navigateurs

En octobre 2017, toutes plates-formes confondues[17], les parts de marché[18] des principaux navigateurs, exprimées en nombre de pages vues, sont **en France** de 48,9% pour Chrome, 22,2% pour Safari, 13% pour Firefox, 4,9% pour Internet Explorer et 3,4% pour Edge.

Les éditeurs de ces navigateurs sont des sociétés et une fondation (Mozilla) dont les sièges sont tous aux Etats-Unis. Les éditeurs européens sont faiblement représentés : la part de marché d'Opera de la société norvégienne Opera Software, qui est le navigateur européen le plus utilisé est de l'ordre 2,6% en Europe.

Les cookies sont des fichiers qui peuvent être stockés sur le navigateur et lus par les sites internet. Le dépôt de ceux qui sont nécessaires à la fourniture du service, tels que les cookies de session ou les cookies d'équilibrage, ne requièrent pas de consentement. Selon le projet de règlement, il en est de même pour les cookies d'audience. Une extension du périmètre de ces exceptions a été proposée par le parlement européen (voir annexe 4, article 8.1.d, 8.1.d bis, 8.1.d ter). Les autres peuvent être classées selon différentes finalités :

- pour améliorer la fluidité de la navigation ou la qualité de l'expérience utilisateur, personnaliser l'accès au site en fonction de la navigation (pages préférées), proposer des services (recommandation) et plus généralement gérer l'offre de service et la relation client (CRM) ;
- pour répondre aux besoins de la publicité, ciblée ou non, selon des paramètres techniques (cookies de limitation d'envoi de bannières, tags de lecture, etc.), comportementaux (qui ne permettent pas d'identifier directement l'internaute) ou personnalisés.

Il existe également d'autres traceurs qui s'appuient, comme les cookies, sur l'enregistrement ou la lecture d'informations sur les navigateurs ou sur les caractéristiques du navigateur et du poste de

[17] Tablettes, smartphones et ordinateurs

[18] Source : Statcounter

travail, telles que les balises web, les *tags* ou le *fingerprinting*. Une balise web est un moyen, généralement invisible, utilisé sur les pages Web ou dans les courriels pour vérifier qu'un utilisateur a accédé à certains contenus. Les utilisations courantes en sont le suivi des courriels et le marquage des pages pour l'analyse Web. L'empreinte digitale d'un navigateur *(fingerprinting)* est une information agrégée (par exemple celle concernant la taille et la résolution de l'écran, les polices de caractères utilisées, etc.) qui peut être utilisée pour identifier complètement ou partiellement un utilisateur.

Qu'il s'agisse de cookies, de balises ou de tags, les internautes font rarement la différence entre un dispositif de gestion technique, nécessaire par exemple à la navigation d'un site marchand pour mettre à jour son panier, et un dispositif de profilage ou de ciblage publicitaire.

Il existe des techniques qui permettent de contrôler l'utilisation des cookies par les sites. Sans que la liste en soit exhaustive, ces techniques comprennent :

- le signal Do Not Track, contenu dans la requête de connexion, par lequel les navigateurs peuvent demander aux sites distants de ne pas tracer l'internaute ;
- l'interdiction des tous les cookies ;
- l'interdiction des cookies déposés par les tierces parties ;
- la navigation privée ;
- l'interdiction, domaine par domaine, des cookies figurant sur des listes noires.
- l'autorisation, domaine par domaine, des cookies figurant sur une liste blanche.

Il est également possible, en s'appuyant sur des listes noires, de restreindre l'accès à des sites ou inversement, de débloquer l'accès à un site dès lors qu'il figure sur une liste blanche.

La diversité des solutions proposées aux internautes pour fixer les paramètres de protection va bien au-delà de la distinction entre cookies first ou tiers. Dans le paragraphe 5, les moyens utilisés par Chrome, Firefox, Internet Explorer et Safari pour protéger la vie privée sont passés en revue. Pour compléter le panorama des solutions techniques existantes, des outils complémentaires comme les bloqueurs de publicité sont également étudiés. **Ces solutions sont pour la plupart récentes et en évolution. La revue du paragraphe 5 met en évidence l'intérêt d'une approche réglementaire technologiquement neutre.**

3.2 L'univers des apps

Le mobile représente aujourd'hui une part croissante des audiences et la majorité des investissements publicitaires dans le numérique : le chiffre d'affaire de la publicité sur mobile devrait dépasser celui du fixe en 2019 (voir § 6.1).

Il existe plus de 2 millions d'applications disponibles sur Apple store[19] et environ 2,8 millions sur Google Play store. Les revenus générés par ces applications sont très significatifs : 11 Md$ pour le magasin d'Apple au troisième trimestre 2017 et 6 Md$ pour Google Play store. La progression des téléchargements est forte pour les deux magasins : entre juin et septembre 2017, 8 milliards d'applications ont été téléchargées sur Apple store (+8%) et 18 milliards sur Google Play store[20] (+10%).

[19] Source : Statistica

[20] Source : Clubic, http://www.clubic.com/application-mobile/actualite-837844-app-store-rentable-google-play.html

En France, un utilisateur[21] dispose en moyenne de 90 applications installées sur son smartphone. Il en utilise 30 par mois et 9 tous les jours. Le temps passé sur ces applications est d'environ 100 minutes par jour (195 minutes en Corée du Sud).

A rebours de ce foisonnement, en Chine, la plate-forme WeChat de Tencent, qui revendique plus de 900 millions d'utilisateurs est devenue un portail de services. Initialement plate-forme de messagerie mobile pour envoyer des messages, téléphoner ou organiser un rendez-vous, cette application s'est diversifiée. Elle sert à payer ses courses ou des services, réserver un billet de train ou de cinéma, etc.

Un utilisateur qui veut activer une application effectue une démarche volontaire, par laquelle il télécharge l'application et en accepte les Conditions Générales d'Utilisation (CGU). Avec le RGPD, lorsque le consentement constitue la base légale du traitement de données personnelles, l'éditeur de l'application devra en outre le demander de manière spécifique. Plusieurs études montrent (c'est le paradoxe de la vie privée), que les internautes sont plus facilement enclins à donner leur consentement dans un tel cadre qu'à l'occasion d'une navigation libre sur le web.

Le format de la publicité pour applications mobiles est adapté à cet univers. Les cookies y sont remplacés par un identifiant[22] de publicité unique et spécifique au terminal : IDFA pour les smartphones et tablettes Apple et AAID pour les équipements Android. Cet identifiant, renouvelable à tout moment à la demande de l'utilisateur (pour iOS et certaines versions d'Android), est accessible via une application. Ils sont utilisés pour constituer des profils publicitaires, pour déterminer si une annonce a déjà été diffusée à un utilisateur spécifique ou limiter sa fréquence d'envoi. Cet identifiant présente l'avantage de pouvoir être géré séparément des autres paramètres de l'équipement et par exemple de pouvoir être remis à jour à la demande de l'internaute, sans l'obliger à réinitialiser les applications qu'il utilise. Cette fonctionnalité permet de séparer la gestion de la pression publicitaire des autres paramètres d'accès aux données de l'internaute[23].

Des enjeux spécifiques sont liés aux équipements mobiles. Ils concernent la possibilité de géolocaliser les utilisateurs au moyen des composants GPS ou des réseaux auxquels ils peuvent se connecter (réseaux des opérateurs de télécommunications ou réseaux Wifi ouverts). Les informations de géolocalisation utilisées conjointement avec d'autres métadonnées comme l'adresse MAC[24] ou l'identifiant de publicité permettent par exemple de mesurer le temps passé dans un magasin, de savoir le nombre de visiteurs ou les zones les plus fréquentées.

Apple a fait le choix par défaut d'activer le service de géolocalisation mais de ne pas autoriser les applications à y accéder. Pour ce faire, l'utilisateur doit donner une autorisation spécifique à chaque application. Pour Android les autorisations d'accès aux données sont octroyées à l'application lors de son installation.

Dans l'univers des apps pour smartphone, un enjeu particulier de la protection de la vie privée est la gestion des autorisations accordées à chaque application pour accéder aux ressources du smartphone (identifiants, géolocalisation, Wifi, carnet d'adresse …).

---

[21] Décryptage des habitudes d'utilisation des consommateurs, App Annie, mai 2017

[22] Un identifiant publicitaire pourrait être créé pour d'autres équipements, ce qu'a fait Microsoft pour Windows 10

[23] C'est le cas pour l'IDFA, cela dépend des versions d'Android pour l'AAID

[24] Il s'agit de l'adresse de niveau 2 (« la couche réseau physique ») des composants Wifi. Chaque terminal Wifi quel qu'il soit, est identifié par une adresse MAC unique.

3.3 Les assistants numériques

Le paramétrage des fonctions d'accès aux données personnelles de l'internaute peut être dissocié des applications. On peut noter que Microsoft propose aujourd'hui[25] avec Windows 10 un paramétrage des catégories principales d'informations collectées : position géographique (affecte l'ensemble des applications et pages web), reconnaissance vocale lors de l'utilisation de Cortana, données de diagnostic (usages applicatifs, logiciels lancés, historique web et données liées à la frappe au clavier…), personnalisation de l'expérience d'utilisation grâce à ces données et publicités personnalisées. C'est alors au niveau du système d'exploitation lui-même que sont proposés les paramètres de protection de la vie privée. La situation est analogue avec iOS (voir § 4.2.2).

Une étape est franchie avec les technologies utilisant l'intelligence artificielle, qui permettent de traiter les demandes des internautes et de leur proposer une réponse ou un service sans le renvoyer à une navigation ou à l'utilisation de plusieurs applications communiquant mal entre elles.

Ce besoin d'**un intermédiaire qui gère une navigation perçue comme trop complexe** explique la montée en puissance des assistants numériques. Selon Tractica[26], 500 millions de personnes utilisaient une forme d'assistant personnel numérique en 2016, et ils pourraient être 1,8 milliards en 2021 (hors marché professionnel). Siri (Apple), S-voice (Samsung), Cortana (Microsoft), Alexa (Amazon), Allo ! Google … ces assistants se déclinent sur tous les terminaux, qu'ils peuvent relier via des équipements dédiés (enceintes connectées) comme Google Home ou Amazon Echo. Ils disposent d'une interface permettant de conduire une conversation en langage naturel, par texte ou par la voix (agents conversationnels ou chatbots), et d'algorithmes permettant de mobiliser toutes les ressources du net en back office. Avec la croissance de leur usage, ils deviendront des intermédiaires importants entre consommateurs et entreprises[27]. Leur atout sera par exemple d'organiser un voyage mobilisant différents services de transport, des propositions d'hébergement et des suggestions de restaurants et de programme culturel. Avec ces assistants, particulièrement quand ils offrent une interface vocale, les navigateurs et les applications tendent à disparaître de l'univers de l'internaute qui les utilise.

Pour être efficaces, les assistants doivent apprendre. Il faut donc les laisser utiliser les données générées par l'utilisateur dans ses interactions, indispensables à l'apprentissage pour l'intelligence artificielle : historiques de recherches, calendriers, contacts, localisations… ce qui se fait généralement en créant un compte. Les données sont envoyées aux fournisseurs des services en ligne que l'assistant mobilise. Ceux-ci les stockent et les traitent. Ce processus nécessite une technologie robuste, mais aussi des règles équilibrées dans les relations entre l'assistant et les services. L'usage des assistants illustrent le paradoxe de la vie privée : malgré des réserves de principe, les utilisateurs acceptent de leur confier leurs données en échange d'un service jugé de qualité.

Mais les assistants pourraient aussi offrir une protection sur mesure[28], dans le cadre d'un dialogue avec l'utilisateur, en lui permettant d'adapter le paramétrage des autorisations d'accès à ses données personnelles en particulier en fonction de l'évolution de ses préférences au cours du temps.

---

[25] Cela résulte d'une procédure de mise en demeure de la CNIL

[26] https://www.tractica.com/research/virtual-digital-assistants/ Août 2016

[27] Livre blanc « les assistants virtuels réorganisent nos vies et redéfinissent le marketing numérique », Bing et iProspect

[28] Privacy? I Can't Even! Making a Case for User- Tailored Privacy Bart P. Knijnenburg | Clemson University

Les assistants personnels, particulièrement ceux qui opèrent via une interface vocale, sont une nouvelle génération de logiciels d'accès aux services de communication électronique, s'interfaçant avec navigateurs et applications, qui ainsi disparaissent de l'univers visible de l'internaute.

Pour les assistants personnels, qui ont accès à certaines données à caractère personnel pour l'apprentissage et la fourniture du service, l'enjeu est la maîtrise des informations :

- captées par l'enceinte quand l'écoute est déclenchée ;
- diffusées dans le cloud, qui peuvent être utilisées par des applications tierces mobilisées par l'assistant.

3.4 Le véhicule connecté

Grâce aux données échangées avec les autres véhicules, les infrastructures routières et Internet, les véhicules connectés vont proposer de plus en plus de services, relatifs à la sécurité, à la gestion des flux, ou à l'info divertissement. Ainsi, un système d'appel d'urgence automatique sera mis en œuvre dans tous les véhicules vendus dans l'Union européenne à partir du 31 mars 2018, dans le cadre de l'initiative eCall de la Commission Européenne.

Plusieurs études estiment que les véhicules neufs seront de plus en plus souvent équipés de fonctionnalités connectées, en série ou en option :

- Pour A.T. Kearney[29], en 2020, 75 % du parc automobile possèdera une forme de connectivité ;
- Pour Accenture Strategy[30], en 2025, tous les véhicules neufs seront équipés de fonctionnalités connectées ;
- Pour NTT DATA[31], 90 % des véhicules présenteront une connectivité embarquée en 2020.

Avec l'accroissement du nombre des véhicules connectés, le marché de la donnée constituera un gisement de valeur ajoutée important. Nombre de ces données sont par nature des données personnelles, qui entrent par conséquent dans le champ du règlement général sur la protection des données et dans celui du projet de règlement e-privacy. Il en est ainsi des données et métadonnées suivantes issues du véhicule :

- les données « client » (nom, prénom, adresse, numéros de téléphone, adresses mail, etc.) ;
- les données de géolocalisation ;
- les données techniques liées à l'état du véhicule et des pièces ;
- le numéro de série du véhicule ou tout identifiant unique du véhicule ou d'une pièce ;
- les données d'usage du véhicule liées à l'activité du conducteur ou des occupants du véhicule (par exemple, les données relatives au style de conduite, vie à bord, etc.).

En matière de sécurité et de trafic, il est possible d'anonymiser les données utiles. C'est le cas par exemple des informations relatives à un embouteillage, à la présence de travaux, ou à des places de parking disponibles. Certaines données de sécurité ou de trafic pourraient toutefois ne pas être transformables en données anonymes : c'est notamment le cas lorsqu'un véhicule envoie une information, par exemple à une infrastructure, et que celle-ci doive lui répondre directement.

---

[29] A. T. Kearney, « Connected car: Value chain disruption », 2016.

[30] Accenture Strategy, « Connected vehicle, Succeding with a disruptive technology », 2015

[31] NTT Data, « Connected Car Report », 2015

La directive 2015/962 pour le développement de systèmes de transport intelligents encourage le recours aux données anonymes : « *dans un souci de protection de la vie privée, l'utilisation de données anonymes est encouragée, le cas échéant, dans le cadre des applications et des services STI*[32] ». Le règlement délégué à cette directive affirme en outre, dans son dixième considérant, que « *si le service d'informations doit s'appuyer sur la collecte de données […], il conviendrait que* ***les utilisateurs finaux soient clairement informés de la collecte de ces données, des modalités de cette collecte et d'un éventuel traçage, et des durées de conservation*** *de telles données. Les responsables de la collecte de données […] devraient déployer des* ***mesures techniques appropriées pour garantir l'anonymat des données reçues*** *d'utilisateurs finaux ou de leurs véhicules* ». L'anonymisation constitue un traitement de données personnelles, qui doit donc être conforme aux conditions détaillées dans l'article 6.1 du RGPD.

La plate-forme C-ITS[33] est allée encore plus loin en proposant une infrastructure de gestion de certificats à clés publiques, permettant de protéger dans la durée l'identité du véhicule dans ses échanges avec les autres véhicules et avec les infrastructures routières[34], en la remplaçant par un alias fréquemment renouvelé. Cette technique est appelée pseudonymisation. Il faut toutefois noter que le groupe G29 a publié un avis relativement critique sur ce mécanisme.

Les services fournis dans le cadre d'un service de maintenance, par exemple l'information donnée par un véhicule qu'il y a lieu de procéder au remplacement d'un organe défectueux, relèvent d'une logique différente : le conducteur du véhicule doit donner son consentement à l'envoi des données.

L'exemple de la voiture connectée montre l'intérêt de mettre en œuvre des techniques comme l'anonymisation ou la pseudonymisation.

4 PRIVACY MADE IN USA

Aux Etats-Unis, plusieurs tentatives de réglementation d'une meilleure protection de la vie privée sur Internet, analogues à la démarche européenne, n'ont pas abouti. Le relais est aujourd'hui pris par une démarche active de certaines entreprises.

4.1 L'approche réglementaire américaine, ou l'attrait du vide ?

Plusieurs projets de loi ont été proposés dans les années 2011 et 2012 pour imposer la mise en œuvre d'un protocole Do Not Track dans la relation avec les sites internet, afin de donner aux utilisateurs la possibilité de choisir ou non d'être suivis par des sites tiers lors de leur navigation sur Internet. Ces projets de loi n'ont pas abouti. La Federal Trade Commission (FTC) a publié en 2012 un rapport « *Protecting consumer privacy in an era of rapid change* » recommandant que les navigateurs incluent un « *opt-out* » permettant aux internautes de ne pas être suivis.

En 2014, la FTC a ouvert une enquête sur l'opérateur américain Verizon, qui utilisait des « supercookies » impossibles à supprimer. L'enquête s'était conclue en mars 2016 par un accord prévoyant une amende de 1,35 M$ et une modification des pratiques de Verizon, qui doit désormais obtenir le consentement de l'internaute et lui permettre de le retirer. Cette affaire avait pesé dans

[32] Systèmes de Transport Intelligents.

[33] Plate-forme « Cooperative, Connected and Automated Mobility » de la Commission Européenne

[34] Il est cependant possible de lever cette anonymisation en cas de vol ou de réquisition judiciaire

l'adoption en octobre 2016, par le Congrès américain, de mesures de régulation proposées par la FCC, parmi lesquelles figurait l'obligation de consentement de l'internaute à la revente de ses données par les opérateurs télécoms. En mars 2017, Donald Trump a signé le retrait de ces mesures. Le dossier est désormais transféré à la Federal Trade Commission (FTC).

Ces mesures avaient été combattues par les opérateurs télécoms et le secteur publicitaire, jugeant qu'elles avantageaient les grandes plateformes du net. AT&T, Comcast et Verizon affirment ne pas prévoir de vendre l'historique de navigation des internautes et préconisent une régulation centrée sur la sensibilité des données, plutôt que sur les acteurs qui les collectent.

Il faut cependant noter que la réglementation américaine prévoit des encadrements sectoriels de l'utilisation des données, par exemple dans les domaines de la santé, de la finance et pour les entreprises ciblant les enfants. Il y a aussi des lois au niveau des Etats : la loi Californienne impose aux entreprises qui font de la publicité en ligne de déclarer si elles respectent ou non le Do Not Track. Enfin, plusieurs questions liées à la vie privée[35] sont en cours d'examen par la Cour Suprême des Etats-Unis fin 2017.

Au pays de « Mad Men », le rôle économique de la publicité n'est pas remis en question, même si, face à la montée de l'utilisation des Adblocks, des voix s'élèvent pour mettre en œuvre de meilleures pratiques publicitaires, moins intrusives et plus respectueuses de la vie privée des internautes (voir par exemple l'initiative *LEAN advertising* de l'IAB ou les travaux de la *Coalition for better adds*). Aux Etats-Unis, certains considèrent que **la régulation peut devenir très vite contreproductive sur le plan économique.** C'est le reproche qu'ils adressent à la réglementation européenne depuis 2002.

La publicité est devenue moins efficace en Europe sous l'effet de la réglementation

Goldfarb Avi, Catherine E. Tucker "Privacy Regulation and Online Advertising" Management Science 57.1 (2011): 57-71

Abstract: We use the responses of 3.3 million survey-takers who had been randomly exposed to 9,596 online display (banner) advertising campaigns to explore how privacy regulation in the European Union has influenced advertising effectiveness. This privacy regulation restricted advertisers' ability to collect data on web users in order to target ad campaigns. ***We find that on average, display advertising became far less effective at changing stated purchase intent after the EU laws were enacted, relative to display advertising in other countries.*** *The loss in effectiveness was more pronounced for websites that had general content (such as news sites), where non-data-driven targeting is particularly hard to do …*

One potential asymmetry is across the breadth of content provided by a website. For example, the use of web bugs and cookies is more important for websites that aim for a general or mainstream audience that is not connected with a specific type of product. Someone visiting www.cruise.com is more likely to be interested in purchasing cruises and can be targeted accordingly, but a portal or a news website cannot be sure whether someone visiting its main page is in the market for cruises unless they track whether that consumer is also reading news features on cruises. This means that general or less product-specific websites could find consumer tracking technologies relatively more useful for targeting ads than product-specific websites is supported by external empirical evidence. For example, the E-Soft annual survey (Reinke, 2007) documents that the 100 websites that use the most web bugs have consistently been general interest websites, like Information.com, photobucket.com, flickr.com, and YouTube, as well as various ad networks.

[35] https://www.nytimes.com/2017/07/10/business/dealbook/digital-privacy-supreme-court.html

Au cœur du modèle américain, on trouve également la conviction que les besoins changeant des utilisateurs sont mieux servis par une diversité de solutions innovantes proposées par des acteurs en concurrence que par un encadrement réglementaire. C'est particulièrement visible dans le cas de la démarche d'Apple.

4.2 Quand Apple se pose en champion de l'e-privacy

Depuis quelques années, et plus particulièrement avec le lancement du système d'exploitation pour mobile iOS 11 en septembre 2017, e-privacy est une composante importante de la stratégie d'Apple.

4.2.1 Recueil de données, « *differential privacy* » : une politique affirmée mais peu transparente

Des balises placées dans des messages publicitaires envoyés par Apple sont utilisées pour savoir si ces messages ont été ouverts. Des adresses URL renvoyant vers un site d'Apple permettent de savoir si l'utilisateur ciblé a manifesté son intérêt pour le message en se connectant à l'adresse URL.

En matière de **technologies de suivi (cookies, balises web et pixels tags), la société collecte des cookies pour mesurer l'efficacité de ses publicités** et connaître les parties de ses sites Web les plus utilisées. Les **données collectées sont alors considérées comme des données non personnelles à l'exception des deux cas suivants** : a) lorsque l'adresse IP est considérée par la loi locale comme une donnée personnelle (ce qui est le cas dans les pays de l'Union européenne) ou b) lorsque des données non personnelles et des données personnelles sont associées auquel cas l'ensemble est assimilé à des données personnelles.

Apple utilise des données personnelles pour ses besoins marketing[36] (développer, améliorer ses produits et services, contenus et publicités), **logistiques** (livrer les produits), de **sécurité** (prévention des pertes, lutte contre la fraude), de **communication** (notifications importantes, modifications de conditions et chartes), **d'audit et d'analyse** en relation avec les produits et services de la société. Elle procède également à la collecte et à la divulgation de données, considérées dans leur document comme non personnelles, telles que le métier, la langue, le code postal, l'identifiant unique de l'appareil, la localisation et le fuseau horaire. Les **informations collectées sur les sites Web de la société peuvent être associées à des métadonnées** comme l'adresse IP pour assurer la qualité des services en ligne.

Apple **partage des données personnelles avec des sociétés qui fournissent des services** tels que traitement d'information, extension de crédit, livraison de produits, exécution des commandes, gestion et développement des données client, réalisation d'enquêtes de satisfaction.

Avec le consentement explicite de l'utilisateur, la société peut collecter des informations sur l'utilisation de l'appareil et des applications afin d'aider les développeurs à améliorer leurs applications.

Apple s'engage aussi à communiquer les informations personnelles qui lui sont demandées du fait de l'application de la loi dans le cadre d'une procédure en justice.

Pour **traiter ces données en les rendant anonymes sans en compromettre la valeur**, Apple **met en œuvre une technique d'offuscation** appelée « differential privacy », qui consiste à ajouter un bruit aléatoire à l'information concernant les utilisateurs et leurs usages avant qu'elle soit envoyée aux

[36] L'ensemble de l'analyse se fonde sur les documents publiés par Apple « Engagement de confidentialité du 19 septembre 2017 » et « Sécurité iOS 10 » de mars 2017.

serveurs de l'entreprise. Ainsi, Apple peut constituer des bases de données d'informations sans que les informations spécifiques à une personne puissent être révélées.

Idéalement, les **données privées se trouvant sur les serveurs devraient être protégées de toute attaque**. Mais selon une étude reprise par le magazine en ligne Wired[37], **l'efficacité de la technique de "differential privacy"** dépend d'une variable appelée le paramètre de perte (« privacy loss parameter ») qui **serait d'un niveau faible chez Apple**. En outre**, le code et les valeurs de ces paramètres ne sont pas publics** et peuvent être modifiés à tout moment, rendant ainsi la politique de protection des données personnelles, au regard de ces critères, totalement opaque.

Le système d'exploitation de l'iPhone permet d'interdire l'accès des applications aux données personnelles de l'utilisateur. Par un paramétrage adapté, **l'utilisateur peut accorder ou refuser les autorisations d'accès aux données personnelles suivantes** : contacts, calendriers, rappels, photos, mouvements et activités physiques, service de géolocalisation, bibliothèque multimédia, comptes de réseaux sociaux tels que Twitter et Facebook. L'accès aux composants et services suivants est également contrôlé par le système d'exploitation dans les mêmes conditions : microphone, caméra, homekit, reconnaissance vocale, partage bluetooth. **Par défaut, ces paramètres sont en position « OFF »** (pas d'accès). En outre, si l'utilisateur synchronise ses données dans le nuage d'Apple, appelé iCloud, il peut autoriser des personnes tierces à y accéder.

4.2.2 iOS 11 et *intelligent tracking prevention* : une protection de la vie privé renforcée

Avant la version actuelle du système d'exploitation pour mobile (iOS 11), l'utilisateur pouvait décider a) de bloquer tous les cookies, b) de toujours autoriser et c) de n'autoriser que les cookies « premier » des sites visités. Le **nouvel OS des mobiles Apple apporte des modifications profondes à l'utilisation des cookies**. S'il est toujours possible de les utiliser pour enregistrer des informations de connexion sur les sites les plus visités, leur utilisation pour effectuer un suivi de site à site (« cross-site ») sera limité ou impossible. En effet, avec la limitation à 24 heures de la durée de vie des cookies tiers, **Apple met en place, à travers la fonctionnalité « Intelligent Tracking Prevention », la possibilité de limiter fortement le ciblage** (retargeting) par les sites marchands. Cette **fonctionnalité est active par défaut**.

L'exemple suivant illustre la dynamique de cette fonctionnalité : si un internaute visite le site exemple.com qui exploite le suivi multi-sites, les cookies de ce site seront effacés si, après 30 jours, l'internaute n'a pas revisité ce site. Les cookies tiers sont effacés le jour suivant. En résumé :

- J0 : les cookies tiers sont autorisés (le traçage cross-site est permis) ;
- J+1 : les cookies tiers ne peuvent plus être utilisés ;
- J+30 : les cookies first sont purgés.

S'il visite de nouveau exemple.com, la prévention intelligente du traçage considère qu'il est intéressé par ce site et conserve les cookies first pour une nouvelle période de 30 jours. L'Intelligent Tracking Prevention ne bloque pas l'utilisation des cookies tiers immédiatement après une visite car ils peuvent être utilisés pour se connecter à un autre site (typiquement un compte Facebook, Twitter ou Google).

[37] Wired, How One of Apple's Key Privacy Safeguards Falls Short, 15 septembre 2017, https://www.wired.com/story/apple-differential-privacy-shortcomings. Cet article s'appuie sur les travaux de plusieurs universitaires (University of Southern California, Indiana University, Tsinghua University).

L'annonce de ces nouvelles fonctionnalités a suscité de vives réactions[38] de la part des professionnels de la publicité. Ils soulignent qu'**Apple n'a pas recherché la concertation ni une solution construite sur un standard**, mais a inventé ses propres règles. Selon leurs termes « *machine-driven cookie choices do not represent user choice; they represent browser-manufacturer choice* ». Leur crainte est que le **navigateur Safari,** qui représente le tiers du trafic mobile sur internet, **contribue à renforcer l'attrait des plates-formes avec connexion** (Google et Facebook en particulier) au détriment des éditeurs de contenus.

La politique adoptée par Apple renforce la protection de l'accès aux données personnelles de l'utilisateur mais elle a un impact lourd sur le marché de la publicité digitale et sur les acteurs de ce marché. En outre, Apple peut moduler cet impact en fonction des spécifications techniques qu'il retient et qui continueront à évoluer pour que l'intelligent tracking reste efficace.

Une telle approche ne peut être examinée du seul point de vue de la protection des données personnelles. Il faut également, de par son effet sur le marché, évaluer s'il existe un risque au titre des règles de concurrence.

4.3 Le paradoxe de la vie privée vu des Etats-Unis

Le paradoxe de la vie privée est illustré par une étude[39] conduite auprès des étudiants du premier cycle du MIT. Cette étude constate que malgré des préférences affichées pour la protection de la vie privée, les étudiants acceptent facilement de transmettre des données privées s'ils y sont incités, et qu'ils abandonnent très vite le souci de protection, si en contrepartie de celui-ci la navigation devient moins facile. « *Consumers say they care about privacy, but at multiple points in the process end up making choices that are inconsistent with their stated preferences* ».

Les auteurs concluent leur étude par des remarques à l'attention des pouvoirs publics : *"On the one hand it might lead policy makers to question the value of stated preferences for privacy when determining privacy policy. On the other hand, it might suggest the need for more extensive privacy protections, from the standpoint that people need to be protected from their willingness to share data in exchange for relatively small monetary incentives"*.

Ils ajoutent, que dans tous les cas, il faut prendre garde à une réglementation qui demanderait un effort à l'internaute ou qui rendrait la navigation plus difficile, car elle serait rejetée par les utilisateurs.

5 QUELLES OPTIONS TECHNIQUES ?

On se propose ici de revenir sur les paramétrages avancés des navigateurs des ordinateurs (desktop), les extensions qui leur sont associées (appelées aussi « add-on » ou modules) et d'examiner les possibilités offertes par plusieurs types de filtrage : le filtrage par listes, le filtrage selon la finalité (mesure d'audience, envoi de publicités, personnalisation du parcours, etc.), le filtrage selon les techniques de traçage et la nature des traceurs et le filtrage selon la catégorie des sites. Cette

[38] An Open Letter from the Digital Advertising Community, September 14, 2017

[39] The Digital Privacy Paradox: Small Money, Small Costs, Small Talk. NBER Working Paper No. 23488 June 2017. © 2017 by Susan Athey, Christian Catalini, and Catherine Tucker

analyse permet d'identifier, dans une typologie de solutions possibles, celles qui sont proposées par des éditeurs qui ont tenu compte de contraintes ergonomiques et des attentes des utilisateurs.

Pour l'ensemble de ces moyens, les questions posées relèvent des catégories suivantes :

- la qualité de la protection ;
- l'impact sur les acteurs économiques ;
- l'ergonomie et la fluidité de la mise en œuvre, y compris la possibilité de revenir sur des choix antérieurs.

Les tests sont effectués avec les dernières versions des navigateurs en téléchargeant la page d'accueil du New York Times. Une synthèse des résultats est proposée pour ces différents outils, selon les catégories précédemment énoncées.

5.1 Filtrer au moyen de listes blanches / noires

5.1.1 Mozilla Firefox V 57, une protection par liste d'exclusion avec possibilité d'exception

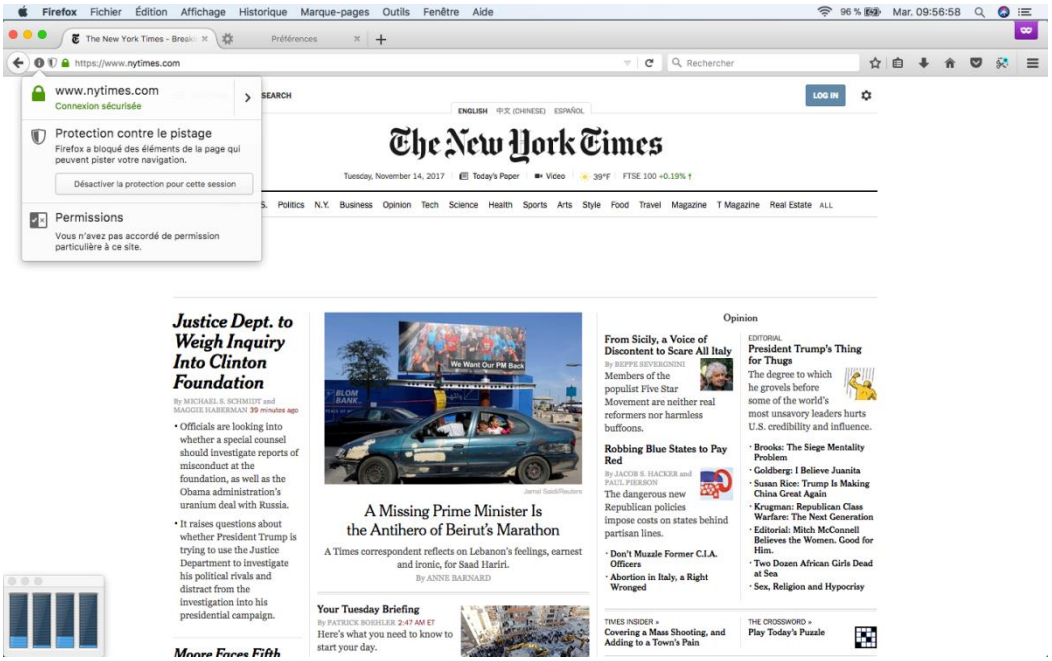
Firefox propose séparément une gestion des cookies, d'activer ou de désactiver Javascript, et une protection contre le pistage. La protection contre le pistage est fondée sur l'utilisation de listes d'exclusion :

- une liste de protection de base qui bloque les « *éléments communément appelés éléments de pistage analytiques, de partage social et de publicité* » ;
- une liste de protection stricte qui bloque « *tous les éléments de pistage connus, y compris les analytiques, ceux de partage social et de la publicité ainsi que des éléments de pistage de contenu* ».

Trois options de protection contre le pistage sont proposées à l'utilisateur : dans le cadre d'une navigation privée, toujours ou jamais. Il est par ailleurs possible de visualiser les cookies et de les supprimer individuellement. Cette fonctionnalité ne supprime pas tous les cookies ; certains cookies (par exemple des cookies d'audience) continuent d'être déposés. Les traceurs publicitaires sont bloqués, mais pas les publicités contextuelles qui continuent d'être servies. La robustesse du dispositif, reposant sur la capacité des listes à filtrer les cookies, est de fait entièrement laissée à l'initiative de Mozilla, l'éditeur de Firefox. La possibilité d'adjoindre une liste personnalisée aux deux listes existantes n'existe pas, mais il existe une possibilité de désactiver la protection par session. Cette fonctionnalité est simple à mettre en œuvre (un clic sur une icône à côté de la barre de menu).

Evaluation des fonctionnalités

- Qualité de la protection : dépend des listes de sites utilisées ;
- Ergonomie et simplicité de mise en œuvre de la protection : **bonne fluidité, peu de clics** ;
- Impact sur les acteurs économique : le passage d'une situation de blocage à une situation d'acceptation du traçage s'effectue en un seul clic. L'information d'acceptation ou d'interdiction ne semble toutefois pas transmise au site visité.



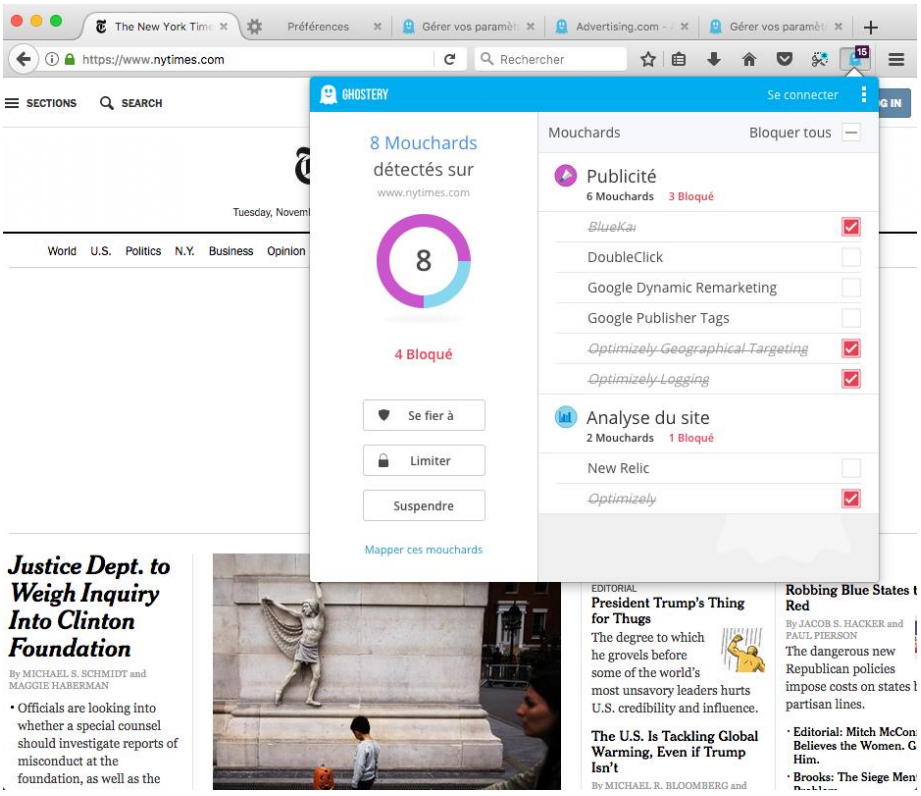
Navigation privée avec Firefox avec possibilité de désactivation de la protection (Cf. menu déroulant en haut à gauche)

5.1.2 Ghostery, une protection fondée sur des listes d'exclusion personnalisées

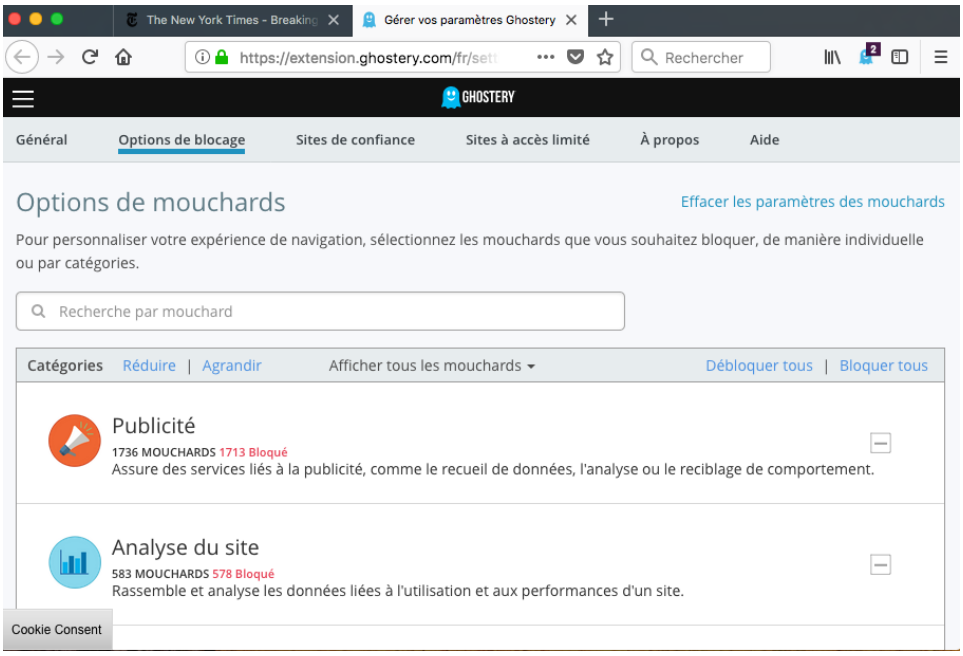
Ghostery est une extension, c'est-à-dire un logiciel compagnon d'un navigateur qui ajoute à ce dernier des fonctionnalités nouvelles. Ghostery a pour objet d'ajouter un niveau de sécurité à la protection des données personnelles de l'utilisateur en filtrant les éléments que les sites peuvent déposer et lire sur son terminal. Pour ce faire, Ghostery répertorie ces éléments (balises, cookies, tags, etc.) et les compare à des listes d'éléments « prohibés ». Ces listes comprennent huit catégories d'éléments : publicité, analyse de site, interactions entre consommateurs, médias sociaux, essentiel, lecteur audio/vidéo, publicité pour adultes et commentaires. L'internaute peut activer ou désactiver chaque liste, et à l'intérieur d'une liste, interdire ou autoriser un site, soit *a priori*, soit pendant la navigation. Pour chaque site visité, Ghostery affiche dans une fenêtre dédiée le nombre d'éléments détectés et parmi ceux-ci les éléments qu'il a bloqués. Ghostery est interactif mais demande un certain niveau d'attention.

Evaluation des fonctionnalités

- Protection : dépend des listes utilisées, a priori forte. P**ossibilité de personnaliser les listes ;**
- Ergonomie : bonne ;
- Impact sur les acteurs économiques : le passage d'une situation de blocage à une situation d'acceptation du traçage s'effectue en un seul clic. L'information d'acceptation n'est pas transmise au site visité. Ce n'est que lors du rechargement de la page que la modification est prise en compte.



Ghostery : les traceurs bloqués et les autres



Ghostery : les listes d'éléments

5.1.3 UBlock Origin, une extension qui filtre les traceurs et bloque des bannières publicitaires

Ublock Origin est une extension s'appuyant, comme Ghostery, sur des listes de traceurs connus. Une interface graphique permet, en désignant un emplacement sur une page, d'accepter les éléments bloqués qui pointent vers cet emplacement. Il s'agit d'un dispositif très efficace qui non seulement filtre les traceurs publicitaires mais bloque les bannières de publicité.

Evaluation des fonctionnalités

- Protection : dépend des listes utilisées, *a priori* supérieure à celles de Firefox et de Ghostery, possibilité de personnaliser les listes ;
- Ergonomie : bonne ;
- Impact sur les acteurs économiques : **possibilité de « débloquer » les éléments pointant sur un emplacement dans une page**. L'information d'acceptation ou d'interdiction ne semble toutefois pas transmise au site visité, il faut recharger la page pour que le choix effectué devienne actif.

UBlock Origin

5.2 Filtrer selon la finalité de ciblage

5.2.1 Le protocole Do Not Track

Les navigateurs mettent en œuvre un protocole particulier appelé « *Do Not Track* ». Il ajoute dans chaque en-tête de requête à un site web (protocole http), un signal indiquant que l'utilisateur ne souhaite pas être suivi. En théorie, les annonceurs et leurs intermédiaires techniques doivent réagir à ce signal en renonçant à cibler l'utilisateur. Celui-ci continuera à recevoir des annonces mais elles ne seront plus ciblées, du fait de l'absence de données comportementales issues de son parcours antérieur.

La difficulté dans l'application de ce protocole est qu'il n'est pas contraignant. Respecter le signal « *Do Not Track* » et ne pas suivre l'utilisateur relève d'une démarche volontaire. Aujourd'hui, des sociétés comme Microsoft, Google, Facebook et Critéo ont déclaré qu'elles ne tenaient pas compte du « Do Not Track » (c'est une obligation imposée par une loi de l'Etat de Californie).

Le Do Not Track est en cours de normalisation au sein du W3C depuis de nombreuses années. Il est passé en *candidate recommandation* en octobre 2017. Le peu d'avancées sur ce dossier explique en partie le succès des extensions aux navigateurs et des orientations prises par certains éditeurs, Firefox en particulier, vers d'autres modes de contrôle des flux publicitaires.

Le groupe de travail des autorités nationales de protection des données d'Europe (G29) encourage les éditeurs de navigateurs à proposer des outils Do Not Track. L'objectif est faire aboutir la normalisation d'un protocole au sein du W3C permettant de recueillir le consentement de l'utilisateur non pas de manière binaire (« Acceptation » ou « Refus » des traceurs) mais plus granulaire (domaine par domaine). Cela permettrait de gérer les exceptions de façon fine et d'enregistrer les préférences de l'internaute pour un domaine particulier, répondant ainsi à la demande des éditeurs.

Evaluation des fonctionnalités

- Protection : dépend du respect du signal Do Not Track ;
- Ergonomie : bonne ;
- Impact sur les acteurs économiques : dépend de la mise en œuvre ou non d'un Do Not Track « granulaire ».

5.2.2 Filtrer selon la finalité des traceurs

Une idée attractive, que l'on retrouve dans de nombreuse réactions[40] au projet de règlement e-privacy, serait de **classer les traceurs en catégories selon leurs finalités**, permettant une distinction plus fine que cookies first / tiers. Ghostery par exemple, classe les cookies en 8 catégories (voir 5.1.2). Ces catégories devraient pouvoir être décrites en des termes simples, facilitant pour chacune le choix d'une option (accepter ou non) par l'utilisateur.

Un classement par finalité serait en particulier intéressant pour créer une catégorie de traceurs utiles au développement d'un service mais qui ne présenteraient pas de problème au regard de la protection des données personnelles (dits *non tracking cookies*). PageFair[41] par exemple, propose que ces traceurs soient traités différemment des autres et donne une série d'exemples tels que :

- permettre à un site web de changer d'apparence lors des différentes visites d'un utilisateur, convertir des prix en monnaie d'origine du visiteur et plus généralement personnaliser la page d'accueil ;
- enregistrer les progrès d'un joueur sans l'obliger à s'identifier ;
- réaliser une campagne de test d'une configuration avec panel de témoins (*A/B testing*) ;
- limiter le nombre de fois où une annonce est présentée à un internaute (*frequency capping*).

La mise en œuvre de cette solution repose sur des choix complexes qui se prêtent difficilement à une définition réglementaire[42] :

- la caractérisation des catégories, leur évolution dans le temps en fonction des pratiques et des technologies ;
- le mode d'affectation d'un traceur à une catégorie et le contrôle de ce mode.

---

[40] C'est la conclusion d'une session de réflexion organisée par le pôle de compétitivité Cap Digital pour la mission, le 8 novembre, avec une trentaine de ses membres

[41] https://pagefair.com/blog/2017/non-tracking-cookies

[42] Le règlement ne distingue aujourd'hui que les traceurs nécessaires au service ou à la mesure d'audience

Comme dans le cas des listes blanches, par exemple, la mise en œuvre de cette solution reposerait soit sur une procédure ouverte, soit sur des choix réalisés par le gestionnaire du logiciel qui proposerait cette option.

5.3 Filtrer selon les techniques de traçage ou la nature du traceur

5.3.1 Google Chrome (V 62.0.3202.89), un paramétrage à trois niveaux

Chrome propose trois niveaux de paramétrage : « Bloquer / Autoriser les sites à enregistrer et à lire les données des cookies » et « Bloquer les cookies tiers ». Il existe également une possibilité de navigation privée à l'issue de laquelle les cookies sont effacés (en plus de l'historique de navigation des données de sites et des informations saisies dans les formulaires). Chrome ne permet pas, pendant une navigation privée, de consentir par exception, au moyen d'une action simple, au dépôt et à la lecture de cookies.

Il est possible d'activer ou de désactiver Javascript et de gérer l'accès des applications aux équipements accessoires de l'ordinateur (micro, caméra). Il existe également une protection contre les accès malicieux.

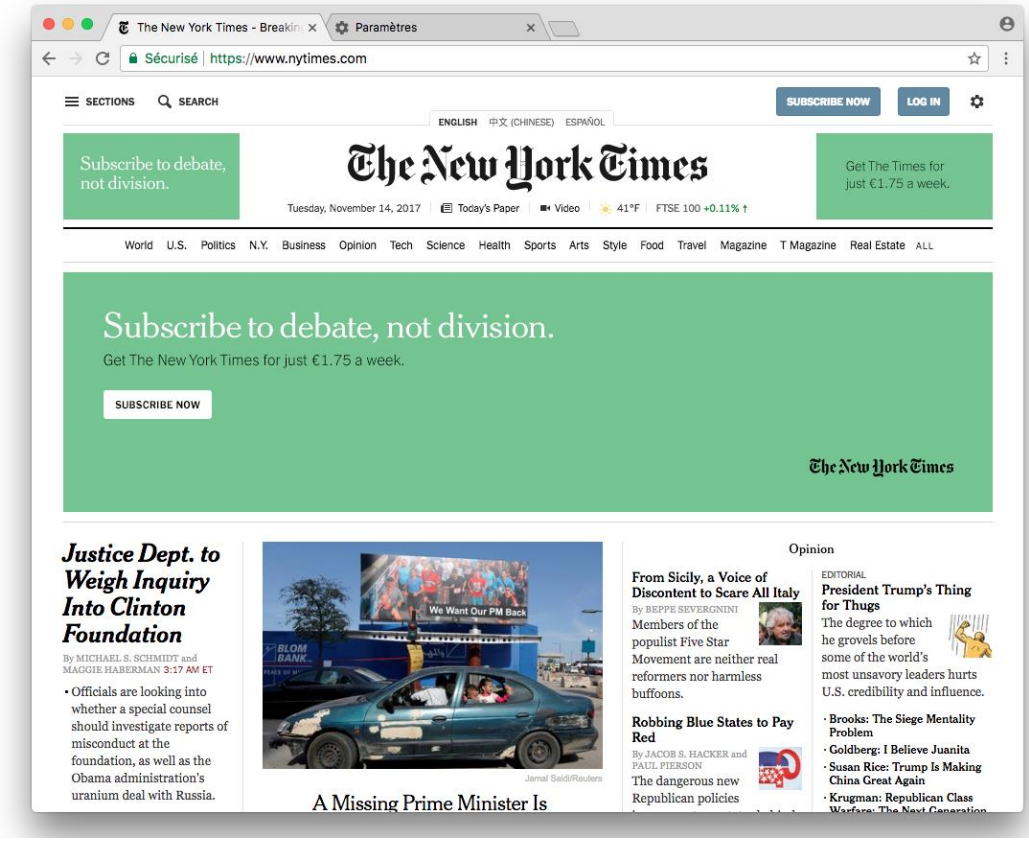
La liste des cookies présents sur le terminal est accessible, mais n'est pas mise à jour de façon dynamique. Il faut relancer la commande d'accès aux paramètres avancées puis aux cookies pour la mettre à jour, c'est une lacune importante de cet outil. A l'usage on constate que les cookies ne sont pas tous bloqués pendant la navigation privée, mais la mission n'a pas eu le moyen de déterminer lesquels ni pourquoi. En revanche, certaines bannières semblent effectivement bloquées.

Le paramétrage de Chrome s'adresse à un public censé connaître l'utilisation des cookies et la façon de les paramétrer. Dans la réalité, les paramètres par défaut sont utilisés par une majorité d'utilisateurs : les cookies sont autorisés pour l'ensemble des sites. Il n'existe pas un moyen d'interagir simplement et de façon dynamique avec l'utilisateur.

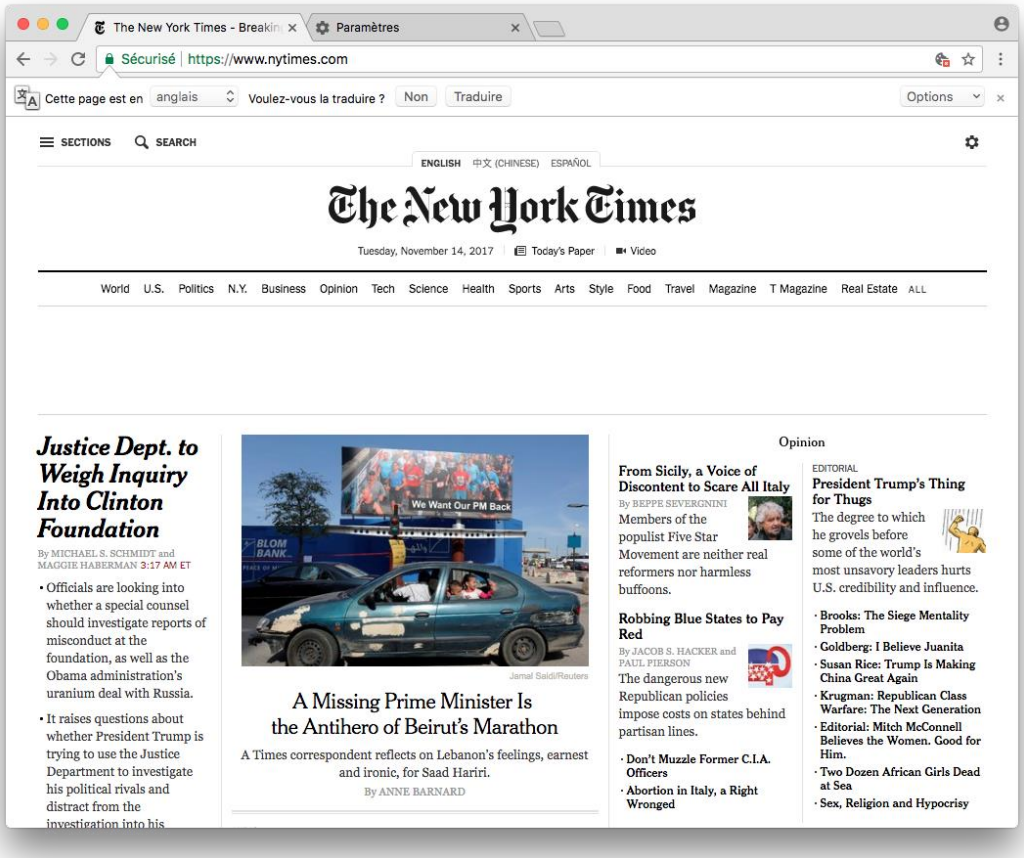
Google a annoncé qu'une version de Chrome dotée d'un dispositif de blocage des publicités non conformes aux règles de bonnes pratiques de la « Coalition for Better Adds » sortirait en 2018.

Evaluation des fonctionnalités

- Protection : fondée sur l'acceptation ou le refus de cookies. A priori moins fine qu'une protection fondée sur des listes d'exclusion ;
- Ergonomie : la modification des paramètres passe par les menus du navigateur. Cette opération est moins fluide (plusieurs clics) que celle permise par Firefox ;
- Impact sur les acteurs économiques : pas de modification (acceptation ou blocage des éléments) « à la volée ». Le retour au menu de paramétrage du navigateur est nécessaire.



Navigation avec Chrome : tous cookies autorisés



Navigation avec Chrome : tous cookies bloqués

5.3.2 Apple Safari Version 11.0.1

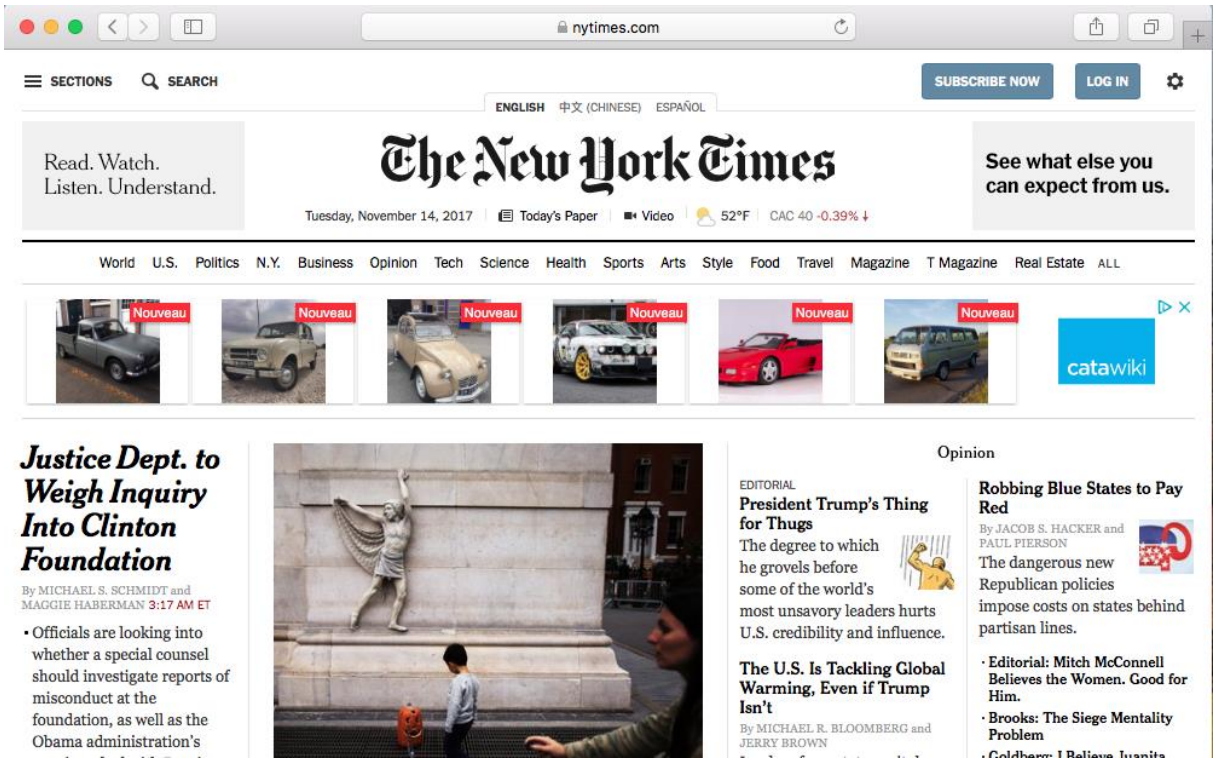
Safari offre une protection des données personnelles qui s'appuie sur la gestion des cookies par nature (premiers/tiers) ou le Do Not Track. Les options proposées sont :

- empêcher le suivi sur plusieurs domaines (effacer régulièrement les cookies tiers) ;
- demander aux autres sites web de ne pas me suivre (Do Not Track) ;
- bloquer tous les cookies ;
- pour tout accepter, il faut décocher toutes les cases.

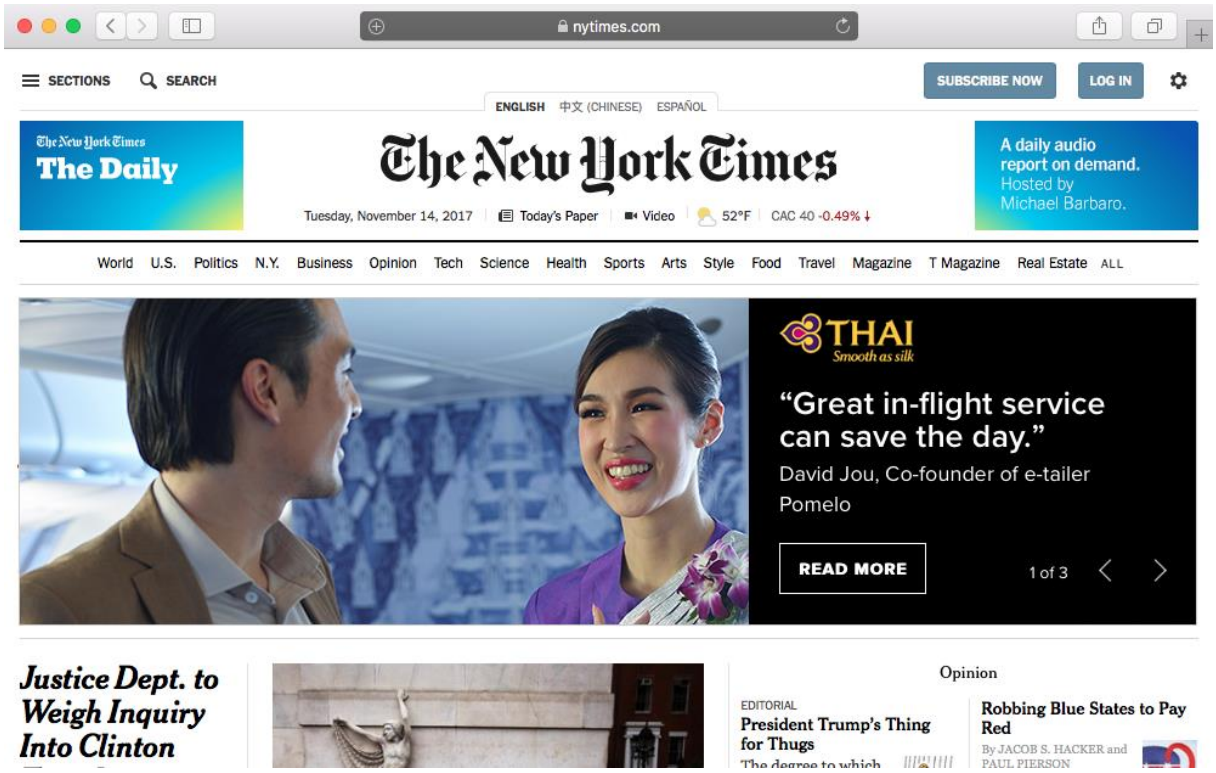
En complément, il est proposé d'activer ou de désactiver Javascript. L'effet constaté de ces options est gradué : les options étant toutes souscrites, seuls des caches sont présents sur le navigateur ; Javascript étant activé, la liste des caches présents s'agrandit et comporte en particulier des caches de suivi d'audience. En autorisant le dépôt des cookies, la liste des données stockées sur le navigateur s'agrandit d'un nombre important de trackers. Enfin, en autorisant le suivi sur plusieurs domaines, le ciblage publicitaire des internautes est sensiblement renforcé.

Safari, propose également une navigation privée dont il est précisé qu'une fois la fenêtre fermée, les cookies, les pages consultées, les informations de remplissage automatique et l'historique des recherches ne seront pas conservées. Des bannières de publicité de nature contextuelle sont servies pendant la navigation, sous réserve que le paramètre de l'option Javascript ait été activé.

Safari, comme Chrome, ne dispose pas d'un moyen simple d'accepter ou de refuser les cookies « à la volée » pendant la navigation privée. Il est nécessaire pour cela de reconfigurer les paramètres de confidentialité via le tableau de bord.



Safari en mode navigation ouverte : suivi intersites autorisé, cookies autorisés



Safari, navigation privée

Evaluation des fonctionnalités

- Protection : fondée sur l'activation de l'une des trois options (effacer les cookies tiers, Do Not Track, bloquer tous les cookies). *A priori* moins fine qu'une protection fondée sur des listes d'exclusion ;
- Ergonomie : la modification des paramètres passe par les menus du navigateur. Cette opération est moins fluide (plusieurs clics) que celle permise par Firefox ;
- Impact sur les acteurs économiques : pas de modification (acceptation ou blocage des éléments) « à la volée ». Le retour au menu de paramétrage du navigateur est nécessaire.

5.4 Filtrer selon la nature des sites

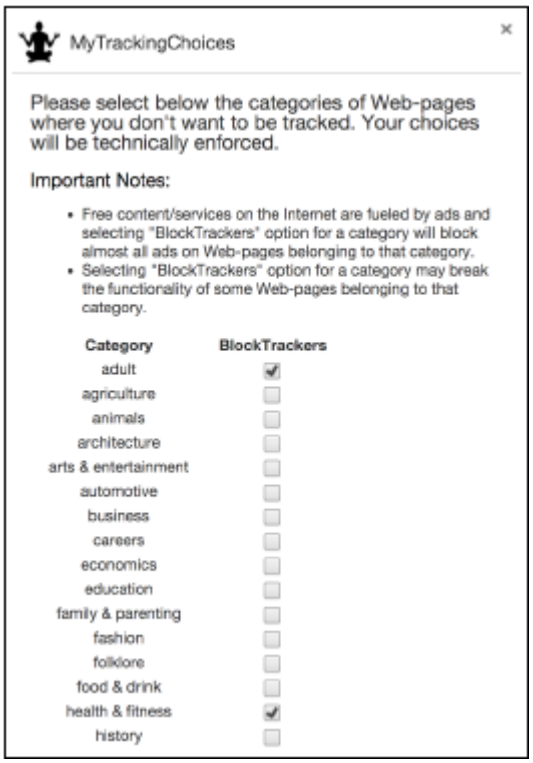
L'INRIA a développé une approche de filtrage différente de celles exposées précédemment. Elle cible les utilisateurs qui ne sont pas contre les publicités mais qui les bloquent pour des raisons de confidentialité. Elle repose sur l'hypothèse que les internautes ne veulent pas être suivis sur des sites web « sensibles » (par exemple liés à la religion ou la santé), mais acceptent d'être suivis et de recevoir des annonces sur les sites moins sensibles (comme les sites d'information ou de sport). En pratique, il s'agit donc de fournir aux utilisateurs la possibilité de spécifier les catégories de pages Web sur lesquelles ils ne veulent pas être suivis et recevoir de cookies tiers.

Le projet s'efforce de trouver un compromis entre le respect de la vie privée et les besoins de l'économie du Web. Pour cela, l'INRIA a développé une extension pour Google Chrome appelée « *MyTrackingChoices* ». Pendant que les utilisateurs naviguent sur le Web, l'extension catégorise les pages Web visitées et, selon les choix de l'utilisateur, elle bloque les connexions réseau des domaines tiers non désirables présents sur la page. Outre le suivi qui est empêché, les annonces des sites tiers

ne sont pas affichées. Raffinement supplémentaire, l'extension fonctionne sur la base des pages visitées et non de la totalité du site.

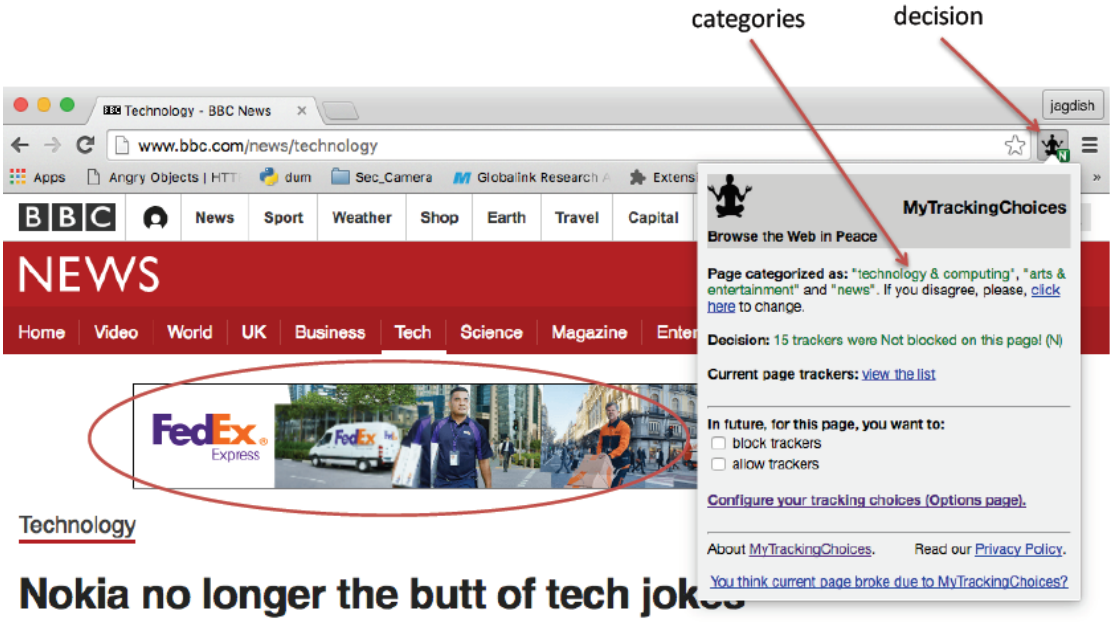
Il convient de noter que, contrairement aux autres bloqueurs de publicité, cette extension ne bloque pas les annonces diffusées directement à partir de l'éditeur.

Il s'agit d'un travail de recherche qui a fait l'objet d'une publication[43] en 2016.



Le panneau de configuration ci-dessus permet de choisir la catégorie de sites sur lesquels l'utilisateur accepte d'être suivi

Copie de la fenêtre surgissante qui accompagne la navigation. Elle montre les catégories (ici une seule, Health & Fitness) auxquelles appartient la page visitée avec la décision de bloquer ou d'autoriser les traceurs. Les utilisateurs ont la possibilité de bloquer ou autoriser les traceurs la prochaine fois qu'ils visitent la page.



Dans cet exemple, la page appartient à plusieurs catégories

[43] MyTrackingChoices: Pacifying the Ad-Block War by Enforcing User Privacy Preferences. Jagdish Prasad Achara, Javier Parra-Arnau, Claude Castelluccia. 2016

Conclusion : les logiciels évoluent et proposent des fonctionnalités permettant le respect de la vie privée plus riches que la seule distinction entre cookies tiers et first party. Elles reposent sur :

- des listes d'exclusion. Ces listes posent le problème de leur gouvernance. Les plus sophistiquées permettent un paramétrage site par site, ou/et le déblocage à la volée d'un site traceur ;
- le Do Not track et ses variantes (granularité), qui repose aujourd'hui techniquement sur un engagement de respect de la part des sites ;
- Le filtrage des traceurs selon leurs finalités, dont les spécifications techniques restent à définir, et qui poserait des questions de gouvernance analogue aux listes d'exclusion ;
- une solution sur mesure (Apple). A partir de sa compréhension de la manière dont fonctionne le ciblage publicitaire, l'éditeur du navigateur propose une solution de protection optimisée, qui constitue un argument commercial.

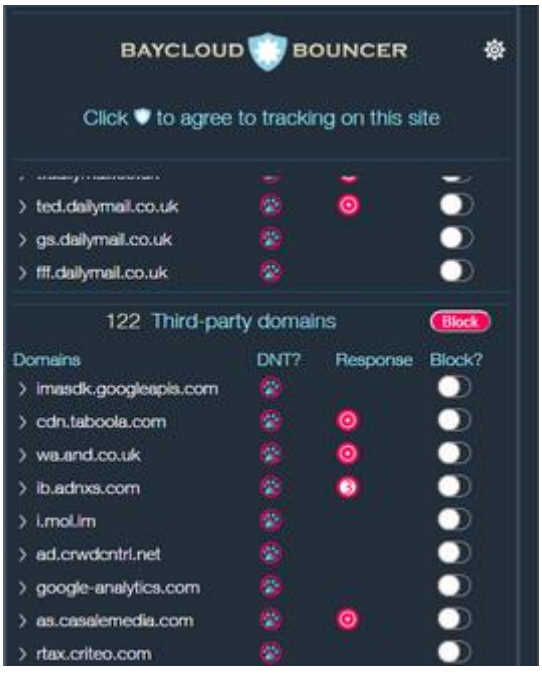
5.5 Gestionnaires de consentement : BayCloud et TartAuCitron

5.5.1 La solution BayCloud

BayCloud est un éditeur fournissant aux entreprises des solutions de protection de la vie privée. Il commercialise en particulier une solution dite « CookieQ » qui permet aux éditeurs de site de recueillir le consentement des utilisateurs avant le dépôt, le traitement ou la lecture des cookies au moyen du protocole Do Not Track.

Le consentement concerne l'ensemble des domaines (hôtes et tiers) de sorte qu'une fois qu'un consentement explicite a été donné à un ensemble de domaines, il n'est pas nécessaire de le demander à nouveau. Les sites peuvent proposer à l'utilisateur de limiter la durée du consentement et de le révoquer à tout moment en cliquant sur l'icône idoine. Le consentement peut être enregistré pour certaines catégories de cookies, tels que « fonctionnel » ou « analytique ».

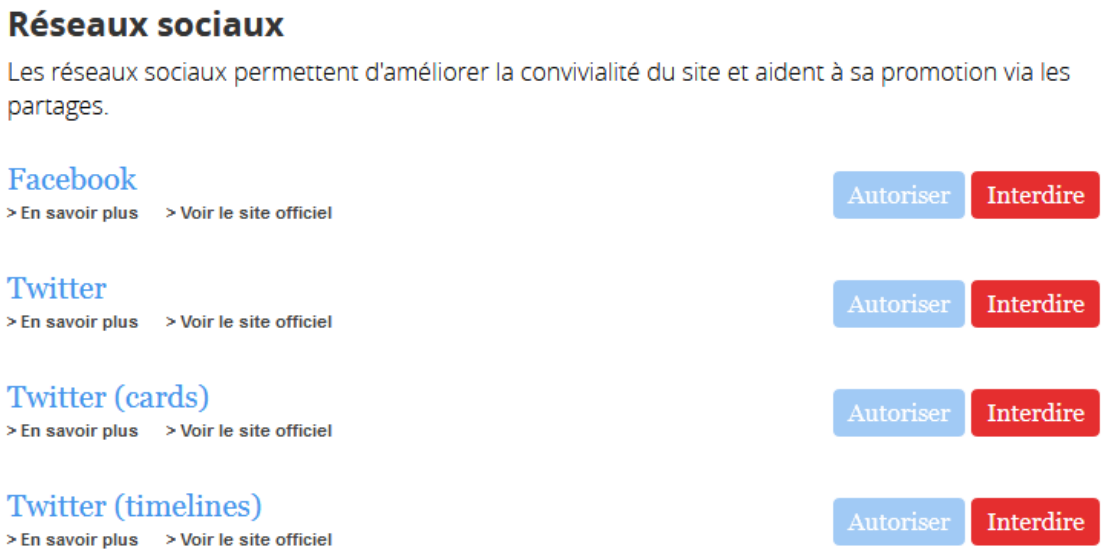
CookieQ peut être configuré pour supprimer automatiquement les cookies first et tiers ainsi que les éléments de stockage pour lesquels le consentement n'a pas été donné ou révoqué.



BayCloud : utilisation du protocole DNT site par site

5.5.2 La solution TartAuCitron

Le logiciel TartAuCitron est mise en œuvre sur le site de la CNIL. Le recueil centralisé du consentement pour différentes fonctionnalités (dépôt de cookies, boutons sociaux, vidéos, autres modules insérés sur les pages du site) s'opère en une seule fois pour la durée prévue par le site.



TartAuCitron : une solution de gestion du consentement centralisée

Conclusion : la gestion du consentement, au moyen d'étiquettes (*tags*), site par site, répond aux dispositions du RGPD et vise aussi le projet de règlement e-Privacy. Mais surtout, elle rend possible le recueil des préférences des utilisateurs dans le cadre d'un dialogue où le site peut expliquer son modèle économique. Cela répond au besoin de transparence et de respect (cf. § 2.2) exprimé par les internautes : quelles sont les données collectées, pour quel traitement et quel usage, et en contrepartie de quel service ? **Contrairement à une gestion centralisée au niveau du navigateur, on initie ainsi un véritable dialogue** par lequel le gestionnaire du site peut expliquer à l'internaute l'effet économique de ses choix.

6 L'IMPACT ECONOMIQUE DU PROJET DE REGLEMENT EUROPEEN

L'analyse de l'impact économique du projet de règlement e-privacy, limité, dans le cas de notre étude, à celui des articles 8,9 et 10, devrait permettre d'estimer l'impact *supplémentaire* que ceux-ci auront par rapport à la réglementation actuelle et à l'entrée en vigueur du RGPD, en mai 2018. L'évaluation réalisée pour la Commission européenne[44] développe une estimation des coûts de mise en conformité selon différents scénarios de propositions de réglementation. Au cours des entretiens menés par la mission, ont été mis en avant trois autres effets économiques sur :

- le marché de la publicité digitale ;
- le e-commerce, le marketing et la relation client (CRM *customer relation management*) ;
- la position concurrentielle des entreprises, notamment vis-à-vis des grandes plateformes internet.

[44] Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector

6.1 Impact sur le marché de la publicité digitale

Selon le baromètre[45] SRI – UDECAM – PWC, la publicité digitale est devenue depuis 2016 le premier secteur publicitaire en part d'investissement dans les médias (33%), devant la télévision. Cette croissance s'est poursuivie (+9,8%) au premier semestre 2017. PWC a transmis à la mission une estimation du marché à l'horizon 2021, qui figure dans le tableau ci-dessous. Le RGPD et sa date de mise en œuvre étaient connus quand elle a été établie, mais e-privacy était seulement à l'état de projet.

Internet advertising in France (US dollar millions) - *Source PWC*

	2016	2019	2020	2021
Mobile internet advertising				
Mobile other Display Internet advertising in France	316	560	617	672
Mobile video Internet advertising in France	175	445	503	560
Mobile paid Search Internet advertising in France	908	1 709	1 897	2 011
Total Mobile internet advertising in France	**1 399**	**2 713**	**3 017**	**3 243**
Wired internet advertising				
Classified Internet advertising in France	495	584	612	638
Other Display Internet advertising in France	554	463	455	451
Video Internet advertising in France	288	390	414	438
Paid Search Internet advertising in France	1 186	796	765	757
Total Wired internet advertising in France	**2 522**	**2 232**	**2 247**	**2 283**
Total Internet advertising in France	**3 922**	**4 946**	**5 264**	**5 526**

Selon cette prévision, la croissance du marché de la publicité digitale devrait être portée par le marché mobile. Une évolution parallèle est également attendue en Europe et aux Etats-Unis.

Le succès du digital vient de ce qu'il a permis aux annonceurs de basculer du **média planning** à **l'audience planning**, c'est-à-dire à des campagnes conçues selon le profil des individus auxquels on va envoyer le message publicitaire. Cette tendance se poursuit avec la **personnalisation**, qui vise à délivrer un message ou une offre individualisés, adaptés à un internaute ou à un groupe particulier. On parle aussi de **publicité comportementale** (OBA, online behavioral advertising), construite sur le profil d'un individu ou d'un groupe d'après leur localisation, l'historique de leurs recherches, et plus généralement la collecte et le traitement de leurs traces de navigation. Comme, sur Internet, toutes les grandes marques sont devenues des médias (via leurs sites, les réseaux sociaux etc.), la publicité rejoint alors la relation client (CRM, customer relation management).

Toutefois, dans les analyses, il n'est pas toujours possible de distinguer clairement les cas où la publicité numérique s'appuie sur des données relevant du RGPD ou de e-privacy (comme la publicité comportementale), des cas où à l'inverse elle n'en relève pas (certaines publicités contextuelles par exemple).

[45] Obsepub, (SRI, PWC, Udecam), 17ème édition et 18ème édition du juillet 2017

L'efficacité des recommandations basées sur l'analyse comportementale

Cité lors d'une audition menée par la mission, l'exemple ci-dessous permet d'illustrer l'efficacité du ciblage comportemental pour proposer des recommandations :

Sur un site média, un test a été conduit au cours de l'été 2016 pour comparer la performance d'une suggestion d'articles de news produite en interne (contextuelle, basée sur des règles simples de proximité sémantique entre les tags utilisés pour qualifier les articles), avec celle d'une recommandation d'articles calculée par un acteur tiers, sur la base du comportement des utilisateurs (et donc faisant appel à des cookies tiers et à des algorithmes).

Sur la période du test (1 mois ½) et à contexte équivalent (même emplacement, même design du bloc), ont été observés :

- un taux de clics enregistré sur les suggestions contextuelles (donc sans cookie tiers) de 1,3% ;
- un taux de clics enregistré sur les recommandations algorithmiques (donc avec cookie tiers) de 2%.

Il s'agit d'une moyenne sur un laps de temps réduit. Néanmoins, tout au long de la période un creusement de l'écart entre les deux solutions a été constaté. En conclusion, le recours à un acteur spécialisé dans la recommandation vidéo, basée sur le comportement des utilisateurs et l'utilisation d'algorithmes, permet d'améliorer la performance obtenue, par rapport aux règles actuelles de suggestion de contenus.

Les deux principaux marchés de la publicité digitale sont le Search (moteurs de recherche) et le Display (bannières ou vidéos, sur tous sites dont les réseaux sociaux). Selon les études, le périmètre des autres leviers (affiliation, comparateurs, e-mailing, petites annonces) peut varier, mais ne représente que 10% à 15% du marché.

6.1.1 Le Search bascule sur mobile et fait un appel croissant à l'intelligence artificielle

Le Search (liens payants sur les moteurs de recherche) devrait continuer à représenter la moitié du marché de la publicité digitale. Il est en train de devenir majoritairement mobile, et de plus en plus local. D'après l'observatoire de l'e pub, le Search local (informations proches du lieu de la recherche) génère déjà en France au 1er semestre 2017 le tiers (32%) des recettes du Search mobile.

Comme une personne utilise son smartphone des dizaines de fois par jour, la plupart du temps pour quelques secondes, il faut accélérer la navigation. Google promeut un standard, « *Accelerated Mobile Pages* (AMP) », pour des pages « allégées », notamment en publicité : les sites respectant ce standard sont mieux classés dans les résultats des recherches sur mobile.

Par ailleurs, suite à une recherche, l'extrait optimisé, court paragraphe placé en tête des résultats (dit en position zéro), utilise l'intelligence artificielle pour comprendre le sens de la requête de l'internaute et lui proposer les extraits jugés les plus explicites des pages trouvées. Si la réponse suffit à l'internaute, le moteur de recherche ne renvoie plus à l'ouverture d'une page web.

Google domine le marché des moteurs de recherche français avec une part de 92,04% (référence StatsCounter, octobre 2017) devant Bing (4,99%), Yahoo (2,11%), DuckDuckGo (0,68%) et 0,12% pour les autres moteurs (MSN, Yandex Ru, Qwant, Ecosia, …).

Le ciblage publicitaire du Search s'appuie sur les données recueillies par le moteur de recherche : contextualisation de la recherche mais aussi de l'historique et, pour les recherches locales, géolocalisation (fixe ou mobile). Les moteurs de recherche affichent leurs règles de confidentialité, et prévoient déjà, le cas échéant, le consentement de l'internaute pour le traitement de certaines données. Le recueil de ce consentement sera à l'avenir mieux encadré par le RGPD. Il est possible

que le souci de protection de la vie privée conduise une part croissante d'internautes à vouloir limiter la collecte de leurs données. C'est le pari que fait Qwant, moteur de recherche français qui ne dépose aucun cookie et ne collecte aucune information personnelle. Cependant, chaque internaute utilise régulièrement un petit nombre de moteurs de recherche qui lui fournissent un service indispensable gratuitement.

> **Dans le cadre d'une telle relation, il sera plus facile de recueillir le consentement de l'internaute.**

6.1.2 La croissance du Display (bannières) est portée par les réseaux sociaux

Le Display (bandeaux publicitaires) progresse plus vite que le Search, mais cette croissance est quasi exclusivement portée par les réseaux sociaux.

L'offre publicitaire sur les réseaux sociaux est ciblée sur le profil des internautes ayant ouvert un compte : l'annonceur dispose d'une sélection de paramètres qui peuvent offrir un ciblage très fin[46]. Il n'a pas accès aux données des internautes, mais l'entreprise qui gère le réseau lui garantit que ses publicités seront servies aux seuls utilisateurs correspondant aux paramètres qu'il a choisis.

Il faut cependant noter que le manque de transparence du système est aujourd'hui très critiqué.

Les internautes accèdent aux réseaux sociaux par leur compte personnel. Le recueil du consentement sur l'utilisation des données personnelles de l'internaute se fait aujourd'hui au moment de la création du compte, via l'acceptation des conditions générales d'utilisation. Avec le RGPD, l'éditeur de l'application devra demander un consentement spécifique pour l'utilisation de données personnelles. Cependant, chaque internaute qui choisit de devenir membre d'un réseau social bénéficie d'un service gratuitement (hors formules premium).

> **Dans le cadre d'une telle relation, il sera plus facile de recueillir le consentement de l'internaute.**

Pour analyser la situation du marché publicitaire des bannières hors réseaux sociaux, Il faut distinguer les achats directs auprès du site commercialisant ces espaces publicitaires et les achats dits « programmatiques ». Le programmatique (voir description en annexe 4) est un outil technique de gestion des campagnes publicitaires qui permet de servir les annonces « impression par impression »[47]. Il prend une part croissante du marché du Display. La publicité sur les réseaux sociaux est programmatique, ainsi qu'une large part de la vidéo.

Le programmatique peut servir pour des achats d'espace en directs (achats d'espaces de gré à gré), ou pour des achats aux enchères (RTB, real time bidding) sur une plateforme ouverte. Selon l'IHS[48], la part du RTB au sein du programmatique, qui a cru très fortement, devrait plafonner (moins de la moitié du programmatique). La même tendance est estimée aux Etats-Unis (44% de RTB en 2017 selon e-Marketer).

---

[46] Les catégories sont alimentées automatiquement à partir de ce que les utilisateurs postent à propos d'eux-mêmes

[47] A l'affichage d'une page, le canal technique programmatique sélectionne quelle publicité est affichée, notamment en fonction de données disponibles sur l'internaute qui appelle cette impression

[48] European Programmatic Market Sizing 2015 (September 2016)

Au sein du Display, selon une étude[49] de IHS Markit, 86% de la publicité programmatique utilise des données comportementales, ainsi que 24% de la publicité non programmatique. La publicité utilisant les données représenterait ainsi 10.6 Md€ d'un marché de 16 Md€ du Display en Europe. Avec la croissance du programmatique, ces chiffres devraient passer à 21,4 Md€ d'un marché de 23,5 Md€ en 2020. Ces chiffres sont cohérents avec ceux du marché américain : aux Etats-Unis, le programmatique représentait 73% du Display en 2016 et devrait croître à 85% en 2019 (source eMarketer, avril 2017). L'impact du programmatique est cependant moins important sur le Display hors réseaux sociaux. C'est notamment le cas en France, comme le montre le tableau ci-dessous.

Etude Zenith : advertising expenditure forecast France - septembre 2017 - En M€	2016	2019
Display	1204	1922
Dont réseaux sociaux (100% programmatique)	*453*	*1193*
Display hors réseaux sociaux	751	729
Display programmatique	639	1468
Part du programmatique dans le Display	*53%*	*76%*
Display programmatique hors réseaux sociaux	186	275
Part du programmatique dans le Display hors réseaux sociaux	*25%*	*38%*

D'après cette prévision, à horizon 2019, les sites de contenu, hors moteurs de recherche et hors réseaux sociaux, devraient en moyenne vendre moins de la moitié de leurs espaces publicitaires via des canaux programmatiques, et au sein de ceux-ci, moins de la moitié par enchères en temps réel. Un site qui vendrait la moitié de ses espaces en programmatique, dont 85% en utilisant un ciblage comportemental (selon les données IHS) et l'autre moitié en direct, dont 24% en utilisant le ciblage comportemental (données IHS), aurait alors 50% de ses espaces publicitaires vendus en utilisant des données de ciblage. Il faut cependant souligner que ce type de calcul moyen recouvre une grande hétérogénéité selon la nature des sites.

La valeur d'un espace publicitaire augmente avec les données qui l'accompagnent

Pour un annonceur, un paramètre important pour mesurer l'efficacité d'une bannière est le taux de clic sur celle-ci. Selon l'étude IHS précitée, ces taux sont très différents : 0,7% pour les campagnes pré-vendues, 3,8% (5 fois plus) avec des données comportementales, 6,9% (10 fois plus) pour le reciblage. Tout naturellement, cette différence de taux de clic se traduit par des fourchettes de prix d'espaces publicitaires différentes : CPM (coût pour mille) de 0,4€ à 8€ sans ciblage comportemental, CPM de 1,8€ à 25€ avec ciblage.

D'autres études font état d'un différentiel de prix moins élevé. Une étude de 2014[50] estime qu'une impression accompagnée d'un cookie peut valoir de 60% à 200% plus cher, selon l'ancienneté du cookie (un cookie récent donnant moins d'information).

Depuis 2010, il est possible de refuser (opt-out via une icône AdChoice) la publicité ciblée. Une étude américaine récente[51] analyse la valeur des publicités servies aux internautes en utilisant cette possibilité. Seules 0.23% des impressions sont servies à des internautes américains qui utilisent cet opt-out, mais les annonces correspondantes valent 59.2% moins cher.

[49] The economic value of behavioural targeting in digital advertising HIS Markit 2017

[50] An empirical analysis of the value of information sharing in the market for online content, J.H. Beales and J.A. Eisenach

[51] Consumer Privacy Choice in Online Advertising: Who Opts Out and at What Cost to Industry? Simon Business School Working Paper No. FR 17-19 (21 Aug 2017)

Les personnes auditées par la mission ont communiqué des analyses confirmant l'ordre de grandeur de ces chiffres. Sur une plateforme de publicité mobile, une analyse des achats programmatiques a été effectuée du 19/09/2017 au 03/10/2017 pour estimer l'effet de la nouvelle version iOS 11 d'Apple sur le prix des publicités. Pendant cette période, les prix moyens d'achat d'impressions webmobile sur Safari iOS11 ont baissé de 25% (format pavé), 33% (format interstitiel) et 50% (format bannière) par rapport aux achats effectués sur les versions antérieures de Safari.

Le programmatique et le ciblage ont un coût : on estime que pour 100 € dépensés par un annonceur, 40 € reviennent au site qui affiche la publicité et 60 € aux intermédiaires techniques (source WFA / UDA).

Il faut aussi noter que le ciblage permet de toucher un internaute en le suivant dans sa navigation sur des « pages intérieures » ou sur des sites de faible notoriété, dont le prix des espace est moins élevé, pour lui servir ainsi à moindre coût une publicité ciblée.

Une large partie de la valeur apportée par les publicités ciblées est ainsi captée par l'annonceur (meilleur taux de clic) ou par les intermédiaires techniques, mais la différence de revenu pour les sites de contenu reste significative. Les personnes auditées dans le cadre de la mission ont confirmé que, une fois déduit le coût des intermédiaires techniques, **le prix payé à l'éditeur augmente avec les données**, citant parfois une hausse de 20 à 30% du CPM, parfois un facteur 2 (de 0,5 € à 1 € du CPM).

En-dehors des grands acteurs du marché et de certaines entreprises nées avec le numérique, les sites de contenu ont besoin de faire appel à des sous-traitants spécialisés qui déposent des cookies tiers qui permettent de proposer des publicités ciblées sur leurs pages. Si ces cookies sont refusés par les internautes, cela peut produire deux effets : une perte de valeur pour les espaces « premium » vendus de gré à gré (en programmatique ou non), et un risque de ne plus trouver d'annonceurs pour les autres espaces, qui sont souvent vendus aux enchères sur une plateforme ouverte (RTB). On peut estimer que pour un site qui vendrait la moitié de ses espaces accompagnés d'un ciblage comportemental, dont la moitié en RTB, un quart de ces espaces resterait invendu et le reste subirait une dévalorisation d'un tiers, conduisant à une baisse des revenus totaux de près de 25%.

Il ne faut pas oublier qu'un tel site ne pourrait pas compenser la baisse de valeur de ses espaces en augmentant la pression publicitaire sur ses pages premium, car cela conduirait à une diminution d'audience. Un exemple en a été fourni à la mission par une régie publicitaire. Suite à un dysfonctionnement en 2017 conduisant à une augmentation de la pression publicitaire, le décrochage de l'audience, accompagné d'une montée des adblocks, a conduit à diviser par 2 le volume de publicités servies !

L'évolution du marché de la publicité digitale est déterminée par les annonceurs et les écosystèmes des grandes plateformes numériques, qui jouent un rôle de prescripteur technique. Les autres acteurs, en particulier les éditeurs de presse, n'ont pas un poids ni une expertise suffisants pour peser sur le marché. Ils doivent suivre son évolution, en se regroupant et en s'appuyant sur des acteurs tiers spécialisés[52] s'ils veulent conserver leur autonomie, ou en ralliant l'écosystème des grandes plateformes.

Le risque d'exclusion du marché est important : les annonceurs ont besoin d'une segmentation de l'audience pour limiter la pression publicitaire. Comme une offre ciblée restera de toute façon

[52] Les grandes plateformes numériques occupent une large part de ce marché, mais il existe une offre alternative dynamique qui permet aux éditeurs de contenu de diversifier leurs sous-traitants

abondante via les grandes plateformes, les espaces publicitaires sans données seront de plus en plus dévalués.

6.1.3 La publicité joue un rôle particulier dans l'équilibre économique de la presse

L'étude des modèles économiques de la presse sort du cadre de cette étude. Pour les éditeurs rencontrés dans le cadre de la mission, en particulier pour la presse traditionnelle, le marché publicitaire n'est pas à lui seul une solution : l'objectif est de préserver le métier initial de vente de contenus, en convaincant une partie de l'audience en ligne de prendre une forme d'abonnement. Cette transition est difficile : les revenus digitaux ne compensent généralement pas la baisse des revenus de l'activité « papier », abonnements et publicités.

Les perspectives du marché de la publicité digitale « presse » ne sont pas négatives car ce marché pourrait connaître une certaine croissance, même si elle est moins importante que celle des moteurs de recherche ou des réseaux sociaux, comme le montre le tableau ci-dessous.

Etude PWC GEMO 2016 (en M€)	2016	2019	2020
Publicité presse quotidienne numérique	199	233	245
Publicité dans les magazines grand public numériques	423	590	653
Publicité revues professionnelles numériques	169	213	227
Total publicité digitale presse (Display dont vidéo)	**791**	**1036**	**1125**

L'audience des sites de presse est importante. Facebook (Facebook connect) ou Google[53] (Insights engine project) développent régulièrement de nouvelles offres à destination des éditeurs de contenu. De leur côté, pour garder un accès indépendant aux annonceurs dans les canaux programmatiques, les éditeurs de presse français développent une approche coopérative (La Place Média, Audience square, Gravity) qui prend place à côté des grandes plateformes numériques mondiales.

Traditionnellement, une régie publicitaire commercialise les espaces des entreprises de presse auprès des annonceurs ou de leurs agents de gré à gré (souvent par un canal « programmatique ») et propose les invendus aux enchères via une plateforme ouverte (RTB). Les éditeurs de presse font généralement appel à des tiers spécialisés qui gèrent pour eux le suivi d'audience et le ciblage. Ils utilisent donc aujourd'hui largement des cookies tiers.

Selon une étude réalisée par Monitor Deloitte[54] pour le syndicat de la presse quotidienne nationale (SPQN), 52% des revenus (377 M€) de la presse quotidienne nationale seront issus du numérique à l'horizon 2020. L'étude fait l'hypothèse qu'en 2020, 100% des revenus publicitaires proviendront d'annonces liées à la donnée qui nécessite des cookies tiers. Elle s'appuie par ailleurs sur un sondage réalisé par Deloitte[55] auprès de 6.000 internautes repartis sur 3 pays (Angleterre, France, Allemagne, 2000 personnes dans chaque pays), qui estime que le taux d'acceptation des cookies tiers (88% aujourd'hui) ne serait plus que de 13% si la question leur était explicitement posée. Sur ces bases, l'étude réalisée pour le SPQN conclut à un risque de perte de deux tiers des revenus issus du numérique. Il s'agit clairement d'un scénario de rupture construit sur l'hypothèse que la quasi-

[53] https://marketingland.com/google-publishers-user-data-insights-engine-project-225452

[54] Monitor Deloitte Etude d'impact du projet de règlement ePrivacy 27 Juillet 2017

[55] https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/about-deloitte/deloitte-uk-european-data-protection-tmt.pdf

disparition des cookies tiers du fait de la directive e-privacy entrainerait l'écroulement des recettes publicitaires de la presse en ligne.

On peut tempérer ce scénario :

- le taux actuel d'acceptation des cookies tiers sur les sites internet de la presse quotidienne nationale est de 95%, sur la base des informations fournies par ces sites. Ce taux est meilleur que le taux de 88% issu du sondage Deloitte. Dans le cadre d'un dialogue avec leurs lecteurs, les sites de presse pourraient continuer à obtenir un meilleur taux d'acceptation. Une étude du GFK[56] donne d'ailleurs une prévision de taux d'acceptation du ciblage de 20% en Europe ;
- sans données, les espaces publicitaires premium de la presse conserveront une certaine valeur, même moindre (voir dernier § de l'encart page 40). En revanche, les autres espaces auront beaucoup plus de mal à trouver preneur.

Avec ces hypothèses, on peut considérer que la perte de valeur des espaces publicitaires serait moins importante. Si elle était de l'ordre de 25% (voir § 6.1.2) elle réduirait cependant à néant la perspective de croissance des revenus publicitaires de la presse.

Comme nous l'avons souligné au départ, pour une grande partie des éditeurs de presse, le marché publicitaire n'est pas à lui seul une solution pour assurer la viabilité économique des titres. Une part sensible des pertes anticipées de revenu n'est pas liée à la publicité, mais à la moindre possibilité de suivre les pratiques des lecteurs pour leur proposer des offres d'abonnement adaptées. La connaissance des lecteurs est un sujet stratégique pour le développement de la presse, comme l'est la connaissance de ses clients pour toute entreprise. Dans la mesure où seule une faible minorité de lecteurs est aujourd'hui abonnée, cette connaissance passe par des techniques de ciblage des internautes. Il s'agit là d'une finalité du ciblage différente de la publicité.

> **Les éditeurs de contenu ont besoin d'une technique de suivi individuel de leurs lecteurs pour leur servir des contenus ou leur proposer des formules d'abonnement adaptés.**

6.1.4 Les annonceurs souhaitent plus de transparence

Du côté des annonceurs, il y a une forte demande pour une amélioration de la transparence de la chaîne publicitaire digitale.

Le coût des intermédiaires techniques dans la chaîne de publicité est élevé, 60% selon les chiffres communiqués à la mission par l'Union des annonceurs (source WFA / UDA). C'est aussi l'estimation publiée aux Etats-Unis par l'ANA (association of national advertisers) en 2014. Une étude plus récente de l'ANA[57] montre que la part des intermédiaires peut descendre à 42% sur un échantillon de campagnes, en achat programmatique direct, bien managées par les annonceurs. L'étude souligne que les annonceurs devraient faire un effort pour gagner plus de transparence : *It is therefore recommended that advertisers demand and secure a source of independent transactional information for their buys. One recommended approach is to access and control your programmatic transaction level data — winning bid log data and metadata — to serve as the advertiser's record of transaction (e.g., "programmatic invoices").* L'ANA a lancé en août 2016 un groupe de travail sur la

[56] https://pagefair.com/blog/2017/new-research-how-many-consent-to-tracking/

[57] Programmatic: seing through the financial fog, may 2017

transparence[58], qui a conclu un an plus tard que des enjeux de transparence existent, qui doivent être résolus par une amélioration des contrôles par les annonceurs.

Les annonceurs français regroupés dans l'UDA se sont régulièrement fait l'écho de ce souci de transparence, et dans son éditorial d'octobre 2017, le président de l'UDA en fait un axe fort de l'action de l'association pour 2018.

> **Ce besoin de transparence se traduit par la nécessité de collecter les données permettant de mieux mesurer l'effectivité et l'efficacité d'une campagne.**

En conclusion, le développement du marché publicitaire sur internet est tiré par l'augmentation de l'audience et par la performance des annonces ciblées (publicité comportementale). Les sites de contenu ne jouent pas un rôle de prescripteur pour les annonceurs et doivent s'adapter pour valoriser leur audience, ou courir le risque de voir leurs espaces publicitaires fortement dévalués. Les moteurs de recherche et les réseaux sociaux (Facebook, Twitter, LinkedIn) sont utilisés gratuitement par une large majorité d'internautes. Ils sont donc bien placés pour recueillir le consentement de leurs utilisateurs. Ils pourront donc continuer à vendre leurs espaces publicitaires via des canaux programmatiques en disposant de leurs propres données de ciblage. Ils seront donc peu touchés par le projet de règlement e-privacy et pourront continuer à offrir aux annonceurs des publicités comportementales efficaces. En revanche, les sites de contenu auront beaucoup plus de difficultés pour y parvenir.

6.2 E-commerce, marketing en ligne et relation client

La protection de la vie privée est une dimension importante de la confiance dans l'économie numérique. Par ailleurs, les différences réglementaires entre Etats européens sont considérées comme une des principales barrières au développement d'un e-commerce transfrontière. Aussi, la décision de la Commission européenne de légiférer par règlement pour la protection de la vie privée, parce qu'elle permet une harmonisation, a-t-elle été bien accueillie au départ par les spécialistes du commerce en ligne.

Depuis, une inquiétude se fait progressivement jour sur l'avenir de l'utilisation des technologies permettant le suivi des internautes. Selon l'association européenne du e-commerce EMOTA[59], des traceurs sont utilisés :

- pour la gestion technique : 77% des sites de e-commerce utilisent des cookies, d'abord pour la gestion du panier d'achat, de la langue de l'internaute et de ses paramètres de paiement ;
- pour le marketing : 72% des sites utilisent les données clients (largement collectées via des cookies) pour leur marketing ;
- pour la publicité : un site sur deux génère plus de 20% de son chiffre d'affaire en accueillant de la publicité tierce.

Le premier point (gestion technique) est particulièrement important pour la fluidité de la navigation et la réalisation d'un acte d'achat. Les sites sur lesquels les internautes s'enregistrent ont plus de facilité pour proposer une gestion fluide (qui peut se conclure par un paiement en un 1 clic), ce qui

[58] http://www.ana.net/miccontent/show?id=ii-production-transparency-2017

[59] EMOTA press release 28 august 2017

augmente l'avantage compétitif lié à la taille des plateformes de e-commerce. Sur les 15 premiers sites de e-commerce en France au 1er trimestre 2017 (source Fevad – Médiamétrie), 10 sont des places de marché, c'est-à-dire des plateformes mettant en relation des acheteurs avec des vendeurs tiers. Sur Amazon par exemple, pour 288 millions de références, seules 2,8 millions sont des produits Amazon, les autres sont issues de la place de marché (chiffres publiés lors du salon IRCE 2016).

En outre, le marketing en ligne repose largement sur la personnalisation. Tous les sites de e-commerce, comme les sites de contenu, utilisent les données dont ils peuvent disposer sur les internautes pour personnaliser leur offre, c'est-à-dire pour proposer un produit, service ou contenu adapté aux préférences spécifiques d'un client. La personnalisation commence dès la navigation sur le site, en optimisant le parcours proposé à l'internaute. Qu'il s'agisse de naviguer dans une base de millions de références de produits, de poursuivre un parcours sur un site de contenu, ou d'afficher une publicité ciblée, les techniques sont sensiblement les mêmes. Le site réalise une gestion automatisée de ce qui s'affiche sur la page en fonction de données collectée sur l'internaute.

C'est en particulier le cas pour les *recommandations*, qui se sont généralisées, sur les sites de contenu comme sur les sites de e-commerce, pour suggérer une poursuite du parcours à un internaute. Dans tous les cas, il s'agit de prédire un score d'intérêt de l'internaute pour une série de propositions et de tenir compte de ce score dans ce qui lui est présenté.

Pour les recettes que les sites de e-commerce tirent de ressources publicitaires, la problématique est la même que celle évoquée dans le point 6.1 ci-dessus.

Les plateformes qui bénéficient d'une clientèle régulière auront plus de facilité pour recueillir le consentement de leurs clients. Ce sera plus difficile pour les sites de e-commerce qui servent des clients plus occasionnels.

En l'absence d'une solution simple et fluide, le poids des grandes plateformes, sur lesquelles un grand nombre d'internautes est enregistré, sera encore renforcé.

6.3 Impacts sur la position concurrentielle des acteurs

Début 2017, l'accueil réservé à l'article 10 du projet e-privacy a souvent été favorable, par exemple : "*Ecommerce Europe*[60] *also welcomes the fact that the proposed Regulation will allow consent to be given by browser settings when technically possible, because this will reduce the consumer's consent fatigue and make it easier for online merchants to seek the consumer's consent*."

Cependant, ce premier accueil favorable n'a pas duré, avec la prise de conscience, dès l'été 2017, que "*The major players that develop browsing software (Google Chrome, Microsoft Internet Explorer, Apple Safari) - all established outside of the European Union - would be able to regulate standard access to the terminal equipment by browser setting consent systems, not only for themselves but also for their competitors*[61]*"*.

> **Il convient de bien distinguer, dans le paramétrage d'un logiciel donnant accès à des services de communication électronique, ce qui relève des traceurs utilisés par l'éditeur de ce logiciel, pour ses propres besoins, d'une part, et ce qui relève des traceurs utilisés pour les services auxquels il donne accès, d'autre part.**

[60] https://www.fevad.com/new-proposal-for-a-regulation-on-eprivacy-pros-and-cons-for-e-commerce/

[61] https://www.ecommerce-europe.eu/app/uploads/2017/07/Ecommerce-Europe-Position-Paper-ePrivacy-July-2017-1.pdf

Cette distinction est d'autant plus importante que, si ces logiciels apparaissent aux yeux du public comme des garants du respect des choix de vie privée de l'internaute, ils seront dans une position de confiance privilégiée. Il peut alors exister un risque de conflit d'intérêt entre leur rôle de « gardiens » et leurs activités propres.

Afin de poser les jalons d'une analyse plus concrète, la mission s'est livrée à un examen des enjeux selon les 3 principales options techniques qui ont été relevées au chapitre 5 : filtrer les traceurs selon des listes blanches ou noires, selon les finalités du traçage, ou selon la nature ou les techniques de traçage. Ces options concernent les traceurs utilisés par les services auquel donne accès le logiciel, et non ceux qui peuvent être utilisés par l'éditeur pour ses besoins propres.

6.3.1 Filtrer selon des listes blanches / noires

Aujourd'hui, les éditeurs qui proposent un filtrage par listes utilisent des listes déjà constituées. **Celles-ci ne sont pas vides au départ, car ce serait une solution inefficace pour l'internaute, qui lui demanderait un investissement trop important pour les constituer.** Les listes d'exclusion de sites intrusifs ou dangereux sont établies à partir de connaissances que n'a pas l'internaute. Même si les listes sont modulables individuellement à la demande de l'internaute, ce qui est souhaitable, leur impact économique est important. Il est en effet probable que l'appartenance à une liste aura un effet immédiat pour un site ou une application, et qu'il pourra avoir du mal à la faire modifier par l'internaute.

La première question posée est donc celle de la gouvernance de la liste et de la transparence de cette gouvernance :

- publication des listes, qui peuvent comprendre des milliers d'items ;
- possibilité ou non de contester ou de demander l'inscription dans une liste ;
- protection contre les conflits d'intérêt du gestionnaire de la liste ;
- mode de mise à jour.

Pour être efficace, cette gouvernance ne peut se concevoir que dans le cadre d'un système réactif et agile. Selon les options, elle peut être plus ou moins partagée selon des processus ouverts aux tiers. **La gouvernance des listes donne un pouvoir économique à ceux qui l'exercent.**

6.3.2 Filtrer selon les finalités du traçage

C'est la demande de beaucoup d'acteurs, qui espèrent ainsi permettre à l'internaute de faire des choix informés. En sélectionnant un nombre raisonnable de catégories (8 dans le cas de Ghostery), on pourrait proposer à l'internaute un choix lié à sa perception du caractère plus ou moins acceptable ou au contraire intrusif, de la finalité proposée.

La mise en œuvre d'une telle solution doit résoudre deux problèmes. Le premier concerne la difficulté à définir le contenu des catégories. La pratique de l'A/B testing, par exemple, est considérée par beaucoup d'acteurs du numérique comme un atout naturel du net et une pratique inoffensive si elle est bien encadrée. Pour d'autres, elle relève de la constitution d'échantillons témoins qui requiert un consentement préalable spécifique. A la connaissance de la mission, il n'existe pas aujourd'hui de standard reconnu qui permettrait de définir des catégories qui seraient consensuelles. Le deuxième problème tient à la difficulté d'affecter un traceur à une catégorie, qui nécessiterait la qualification de la finalité du traceur, l'affichage de cette finalité et le contrôle.

In fine, sauf à concevoir la mise en œuvre d'une gouvernance des catégories donnant des garanties d'indépendance, **l'éditeur du logiciel de filtrage prendrait un pouvoir économique** analogue à ce qui est détaillé dans le cas précédent.

6.3.3 Filtrer selon la nature ou les techniques de traçage

La distinction entre cookies first et tiers a permis une première solution de paramétrage des navigateurs, qui existe depuis plusieurs années. Elle a l'avantage d'être à la fois simple et objective, mais elle est largement jugée aujourd'hui trop rudimentaire pour être efficace, comme le montre l'exemple des solutions déployées par Apple. Mais cet exemple montre aussi que l'on perd rapidement en transparence ce que l'on gagne en efficacité ! Sans compter que les spécifications techniques ne sont pas figées : gageons que la solution proposée par Apple (en particulier le paramétrage de l'*Intelligent tracking system*) a vocation à évoluer en fonction des astuces techniques qui seront trouvées par les acteurs de la publicité digitale pour passer au travers des mailles du filet.

Comme on le voit déjà avec les réactions vis-à-vis d'Apple, toute solution « propriétaire » devra être examinée au regard de son effet réel, en pratique, sur les acteurs du marché. En particulier, il conviendra de vérifier que si certains acteurs sont moins pénalisés que d'autres, cela se fait dans de bonnes conditions de transparence et de pratiques commerciales loyales.

> **Cette analyse rapide montre que le paramétrage d'un logiciel d'accès aux services de communication, pour la protection de la vie privée, a le caractère d'un service aux utilisateurs, qui relève de la responsabilité de l'éditeur de ce logiciel.**

Ces logiciels d'accès ou de contrôle d'accès peuvent servir à enregistrer des consentements spécifiques donnés par l'utilisateur du terminal pour un domaine ou un service particulier, mais ils n'ont pas aujourd'hui d'obligation légale et n'en auront pas au titre du RGPD, pour le traitement de données que l'éditeur du logiciel n'effectue pas lui-même, ou qui ne sont pas effectuées pour son compte. **Ce consentement doit être demandé par le responsable du traitement directement à l'internaute.**

Si la gestion du consentement devient une obligation légale des logiciels de contrôle d'accès aux services de communication, et si cela s'accompagne d'une obligation de proposer un paramétrage par défaut refusant tout accès, des interrogations apparaissent concernant les acceptations données au cas par cas par l'internaute :

- concernant les navigateurs, les solutions retenues aujourd'hui par les éditeurs, qui ont choisi ces options pour leur ergonomie, leur simplicité de mise en œuvre et qui intègrent une expertise en matière de sécurité que n'a pas l'utilisateur, deviendraient caduques. Est-il souhaitable d'imposer un système unique ?
- Les systèmes d'exploitation sont aussi des logiciels d'accès. Mais Windows 10, par exemple, ne permet pas de contrôler le paramétrage d'un navigateur qui ne dépend pas de Microsoft. Plus généralement, quand l'accès à un service de communication électronique dépend d'une chaîne de plusieurs logiciels contrôlant cet accès, comme c'est le cas pour les assistants personnels, comment se partage la responsabilité ?

7 PROPOSITIONS

A l'issue des analyses qui précèdent, nous pensons qu'au-delà de la mise en œuvre du RGPD, le projet de règlement e-privacy, tel qu'il est proposé, risque de renforcer la position des grandes plateformes du net qui disposent d'utilisateurs réguliers, dont une large part a ouvert un compte. En revanche, il risque d'affaiblir les acteurs exploitant des services ou sites qui servent des clients occasionnels. S'il impose un paramétrage des logiciels d'accès aux services de communication électronique selon des modalités dont l'ergonomie n'a pas été testée et dont on ne sait pas s'il répond au besoin des utilisateurs, il pourrait susciter une réaction de rejet parmi ceux-ci.

Nous proposons quatre principes qui pourraient guider la réflexion, et inspirer les positions françaises lors de la poursuite de la négociation du texte du règlement.

7.1 Pour préserver la vie privée de façon durable, le règlement doit être neutre technologiquement

Le bref panorama des logiciels d'accès et des pistes de solutions que nous avons décrits dans le rapport montre à quel point l'écosystème est complexe et en pleine évolution.

L'exemple de Safari / iOS 11 montre la richesse et la complexité d'un dispositif de protection de la vie privée, qui sera en outre amené à évoluer. Plus généralement, la variété des marchés (services de communication électronique fixes, mobiles, internet des objets - des montres aux véhicules connectés) et pour chaque marché, la variété des options (paramétrage ou options des logiciels d'accès, installation d'extensions comme un logiciel de protection contre le tracking, un ad-block ou un anti-virus), montrent l'impossibilité de définir des spécifications techniques qui couvriraient un champ aussi large.

En outre, de nouvelles réponses permettant de renforcer le respect de la vie privée émergent via les techniques d'anonymisation (voir l'exemple du véhicule connecté), le développement du « privacy by design » ou des technologies de traitement des données (differential privacy).

Pour garantir que l'accès aux services de communication électronique respecte la vie privée de façon durable dans un environnement évolutif, la rédaction du règlement doit être technologiquement neutre. Elle doit l'être à la fois dans ses articles et dans ses considérants, comme le souligne par exemple la fondation Mozilla dans sa prise de position[62], à propos notamment des considérants 22 à 24. Même si les versions successives du projet de règlement ont plutôt évolué dans le sens de la neutralité technologique, cela reste un impératif.

Recommandation n° 1.	La rédaction du projet de règlement doit être neutre technologiquement, pour l'ensemble du texte y compris les considérants.

[62] https://blog.mozilla.org/netpolicy/files/2017/10/ePrivacy-position-paper-_-FINAL.pdf

7.2 L'offre de logiciels permettant la protection de la vie privée doit continuer à se diversifier et à s'enrichir

La possibilité d'empêcher les tiers de stocker des informations sur l'équipement terminal ou de traiter des informations déjà stockées peut relever d'une fonction proposée par l'éditeur d'un logiciel d'accès à des services de communication électronique ou d'une extension à ce logiciel, qui peut être fournie par une autre société.

La meilleure façon de garantir que les solutions proposées répondent aux attentes diverses des utilisateurs et à leur souci d'ergonomie, est que l'offre de logiciels permettant la protection de la vie privée puisse continuer à se diversifier et à s'enrichir. Pour cela, il faut que les divers logiciels de contrôle d'accès, en particulier les extensions, soient considérées au même niveau que les logiciels d'accès aux services de communication électronique.

Le savoir-faire des éditeurs se traduit par la proposition de scénarios de protection des données des internautes, en explicitant les paramètres de ces scénarios et leurs conséquences et en donnant le choix aux internautes de choisir l'un d'entre eux. L'éditeur doit pouvoir choisir librement les paramètres de ces scénarios, en particulier pour l'option par défaut. Il s'agit d'un service proposé aux utilisateurs.

Ces logiciels d'accès ou de contrôle d'accès peuvent enregistrer les consentements donnés par l'utilisateur du terminal, mais ne doivent pas devenir les opérateurs (au sens de l'article 9.2) de ce consentement, qui en tout état de cause doit être demandé par le responsable du traitement directement à l'internaute.

Recommandation n° 2.	L'offre de logiciels permettant la protection de la vie privée doit continuer à se diversifier et à s'enrichir. Le règlement ne doit pas donner un rôle privilégié de « portier » à certains d'entre eux. Un logiciel d'accès ou de contrôle d'accès aux services de communication électronique doit proposer plusieurs scénarios de protection, expliquer clairement les implications de ces différentes options et offrir un mode opératoire simple pour accepter le paramétrage par défaut, le renforcer ou l'assouplir.

Il convient de bien distinguer, dans le paramétrage d'un logiciel donnant accès à des services de communication électronique, ce qui relève des traceurs utilisés par l'éditeur de ce logiciel, pour ses propres besoins, d'une part, et ce qui relève des traceurs utilisés pour les services auxquels il donne accès, d'autre part. Les éditeurs de ces logiciels se trouvent dans une position particulière : ils doivent recueillir le consentement des internautes pour les données qu'ils utilisent pour leurs besoins propres, alors qu'ils apparaissent comme les garants de la protection de la vie privée de ces mêmes internautes, vis-à-vis des services tiers. Il conviendra de s'assurer que cette situation n'entraine pas de conflit d'intérêt, en particulier concernant l'activité commerciale de ces éditeurs.

Ce point est particulièrement important quand l'éditeur occupe une position dominante sur son marché.

Recommandation n° 3.	L'incidence des options proposées (notamment du paramétrage par défaut) par les logiciels d'accès à des services de communication dont les éditeurs occupent une position dominante sur leur marché devra être examinée par les autorités chargées du respect du droit de la concurrence.

7.3 Pour préserver un Internet ouvert, il faut offrir une « voie de retour »

Les services ou sites qui servent des utilisateurs occasionnels ont un besoin impératif de créer un contact direct avec eux, pour leur permettre d'une part, de personnaliser leur offre de service, ce qui est un des atouts des services en ligne, et d'autre part, de leur présenter les options économiques de la fourniture du service, y compris le financement par la publicité.

Il s'agit d'un dialogue avec l'internaute pour le solliciter, recueillir son consentement et le cas échéant, modifier, pour le site considéré, le paramétrage du logiciel de contrôle qui a permis l'accès au service considéré. Cela constitue une « voie de retour ».

Une solution serait de définir les spécifications fonctionnelles de cette « voie de retour » et de s'engager dans un processus de normalisation internationale pour définir les fonctions qui doivent être offertes par les logiciels d'accès aux services de communication électronique. Ce processus devrait associer l'ensemble des parties prenantes et donner confiance aux fournisseurs de service dépendants de ces logiciels.

L'exemple de l'échec en 2006 du protocole P3P[63] et la lenteur des tentatives de normalisation du Do Not Track au sein du W3C montrent la difficulté de ce type de démarche, dont la réussite dans des délais compatibles avec la mise en œuvre du règlement e-privacy n'est pas garantie.

C'est pourquoi, le projet de règlement doit mentionner la nécessité, pour les logiciels d'accès, de proposer un mode opératoire simple et ergonomique pour corriger leur paramétrage afin de tenir compte du consentement que donnerait un internaute pour un site ou un service particulier.

Recommandation n° 4.	Un logiciel d'accès ou de contrôle d'accès aux services de communication électronique doit proposer un mode opératoire simple pour corriger son paramétrage afin de tenir compte du consentement que donnerait un internaute pour un site ou service particulier.

La question dite du *tracking wall* doit trouver une réponse. Une entreprise doit pouvoir conditionner l'accès à ses services à l'acceptation de différentes conditions (abonnement, publicités …). Il s'agit d'assurer la poursuite d'un dialogue entre le fournisseur et son client sur les conditions économiques de la fourniture du service, et de proposer par exemple un abonnement, un service *premium* contre

[63] http://www.allaboutcookies.org/p3p-cookies/index.html

l'acceptation de publicités ciblées, ou un service basique (*freemium*) sans ciblage, ou toute autre formulation compatible avec le RGPD.

Le projet de règlement e-privacy de la Commission ne fermait pas la porte explicitement à ces options. Comme la proposition du Parlement européen semble vouloir l'exclure, il nous paraît important de réaffirmer qu'elle est nécessaire à la recherche de l'équilibre économique de nombreux sites ou services.

Recommandation n° 5.	Si un fournisseur de service souhaite utiliser, à des fins commerciales ou de développement du service qui ne sont pas strictement nécessaires à la fourniture de ce service, des capacités de traitement ou de stockage des équipements terminaux, il doit pouvoir offrir à l'utilisateur plusieurs options d'accès au service, selon que l'utilisateur a donné ou non son consentement.

Une des caractéristiques du numérique est la « longue traine », c'est-à-dire la capacité à offrir à un très grand nombre d'acteurs petits et moyens un accès aux internautes. Avec le développement des grandes plateformes internationales, qui captent une part croissante de la valeur, la part relative de marché accessible aux acteurs petits et moyens tend à devenir marginale.

Le règlement e-privacy peut être l'opportunité de promouvoir un développement des marchés numériques respectueux des données personnelles. Il ne doit donc pas pénaliser les acteurs européens, acteurs numériques ou entreprises traditionnelles en mutation, dans leurs développements, face aux grandes plateformes numériques internationales, dont aucune n'est européenne. Il ne faut pas davantage les pousser dans les bras des grandes plateformes numériques, au risque de renforcer la position d'oligopole de ces grands acteurs. Comme le montre la mutation du marché de la musique, les acteurs ont besoin de temps et de moyens pour faire évoluer leurs modèles économiques. Ces acteurs s'appuient sur des tiers spécialisés pour accompagner cette évolution délicate, qui ne doit pas être remise en cause par la mise en œuvre trop rapide du règlement e-privacy.

Recommandation n° 6.	Les délais de mise en œuvre du règlement e-privacy doivent être aménagés, particulièrement après que le règlement aura été adopté, pour permettre aux acteurs les plus fragiles de s'adapter.

7.4 Réguler la pression publicitaire sur Internet

La croissance rapide du marché de la publicité digitale n'est pas sans nuages. La pression publicitaire est parfois mal maitrisée, ce qui se traduit par la montée des Adblocks. La transparence du marché pour les professionnels n'est pas toujours au rendez-vous, ce qui se traduit par des dysfonctionnements ou des fraudes (taux élevé de clics sur des publicités par des robots, erreurs de mesure sur le nombre des publicités servies ou vues, …).

Une partie de la perception de la pression publicitaire vient de la réaction des internautes vis-à-vis de publicités jugées invasives, dont certaines, les publicités ciblées, utilisent des données personnelles. Pour autant, **la régulation de la pression publicitaire ne relève pas au premier chef du règlement e-privacy**. C'est aux entreprises de s'organiser pour répondre à la montée des ad-block et améliorer l'expérience de leurs utilisateurs.

C'est une problématique dont l'interprofession publicitaire, par le biais de l'ARPP notamment et de ses membres, s'est déjà emparée. Cela va au-delà de e-privacy, mais **une meilleure image de la publicité auprès des internautes serait de nature à faciliter le recueil de leur consentement pour des publicité ciblées.**

Recommandation n° 7.	Les initiatives d'autorégulation de la publicité par les professionnels devraient être encouragées par les pouvoirs publics.
Recommandation n° 8.	Un programme de contrôle de la transparence de la chaine publicitaire devrait être mis en œuvre par les autorités de contrôle publiques.

ANNEXES

Annexe 1 : Lettre de mission

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

LE MINISTRE DE L'ÉCONOMIE
ET DES FINANCES

LA MINISTRE DE LA CULTURE

LE SECRÉTAIRE D'ÉTAT
AUPRÈS DU PREMIER MINISTRE,
CHARGÉ DU NUMÉRIQUE

Monsieur Luc ROUSSEAU
Vice-président
Conseil général de l'économie
Ministère de l'Économie et des Finances
139, rue de Bercy
75572 PARIS Cedex 12

Paris, le 23 OCT. 2017

Nos réf. : TR/2017/P/25529/CMA

Monsieur le Vice-président,

La Commission européenne a présenté le 10 janvier 2017 une proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques (ci-après « le règlement *e-privacy* »), présenté comme une *lex specialis* du Règlement général sur la protection des données personnelles (RGPD) adopté en avril 2016 et entrant en vigueur le 25 mai 2018.

Ce projet de texte est en cours d'examen par le Conseil des ministres de l'Union européenne (UE), dans sa formation « Transports, télécommunications et énergie ». Au départ, la Commission a affiché son souhait de finaliser les échanges au plus vite pour que ce texte, d'application immédiate dans tous les États membres, entre en vigueur dès le 25 mai 2018, soit en même temps que le RGPD. Les articles 8 à 10 du projet de règlement *e-privacy*, relatifs à l'encadrement des *cookies*, à la définition du consentement et à son recueil *via* le paramétrage du navigateur suscitent de vives inquiétudes tant parmi les représentants de la presse et des médias en ligne que parmi les acteurs de la publicité digitale.

En effet, l'encadrement renforcé prévu dans le projet de règlement pourrait conduire une part significative, voire majoritaire, des internautes à refuser *a priori* certains *cookies*. Or ces derniers sont utilisés aujourd'hui pour la personnalisation du contenu des sites, qui constitue un important facteur d'attractivité du service pour les utilisateurs, et pour la publicité ciblée, dont le développement, conjugué aux progrès techniques dans la gestion des données, laisse présager une amélioration à court terme du modèle économique encore déséquilibré des éditeurs de services en ligne.

Nous vous serions reconnaissants de nous fournir des éléments d'analyse qui permettraient d'apprécier plus précisément l'impact des mesures envisagées dans le projet de règlement sur les acteurs concernés à la fois sur le plan économique (manque à gagner, investissement pour se maintenir ou s'adapter…) et sur le plan technologique, à travers la description des solutions d'adaptations qui pourraient être mises en œuvre, en tenant compte de leur acceptabilité sociale (caractère intrusif ou répétitif) et de leur ergonomie (facilité d'usage).

En outre, vous pourriez notamment éclairer le gouvernement sur :

- le risque de renforcement de la position dominante des acteurs dominants (Facebook, Google) sur le marché de la publicité ciblé;
- les alternatives techniques (ex. extension URL) dont disposent les acteurs pour procéder à de la publicité ciblée sans recours à des *cookies* tiers ;
- l'opportunité d'imposer des obligations différenciées suivant la finalité des *cookies* ; à cette fin, le « filtrage » effectué par les navigateurs des *cookies* selon leur finalité vous parait-il souhaitable et possible ? ;
- l'intérêt d'une promotion voire d'une généralisation sur le territoire de l'Union de la fonctionnalité « *Do Not Track* » du protocole HTTP afin de permettre de recueillir le consentement de l'utilisateur, non pas de manière binaire (« pour » ou « contre » les traceurs) mais granulaire (site par site) ;
- l'identification de mesures techniques alternatives à celles proposées par la Commission européenne, permettant de concilier le respect de la vie privée des internautes et l'intérêt économique des acteurs en ligne.

Compte-tenu du calendrier de la négociation, vous travaillerez en étroite liaison avec les directions de l'administration chargées de l'élaboration des positions françaises, en particulier avec la direction générale des entreprises et le SGAE. Nous vous saurions gré de nous remettre vos principales conclusions d'ici deux mois. Selon ces conclusions, vos travaux pourront faire l'objet d'un rapport publié en français et en anglais.

Nous vous prions d'agréer, Monsieur le Vice-président, l'expression de notre considération distinguée.

Bruno LE MAIRE Mounir MAHJOUBI Françoise NYSSEN

Annexe 2 : Liste des personnes rencontrées ou interrogées

Organismes publics et parapublics

Ministère de la Justice

- Mme Aurélia Schaff, conseillère chargée de l'Europe et des relations internationales
- Mme Pauline Dubarry, bureau de la négociation pénale européenne et internationale, cheffe de bureau
- M. Corentin Hellendorff, direction des affaires civiles et du sceau, rédacteur expert

Secrétariat d'État auprès du Premier ministre, chargé du Numérique

- M. Côme Berbain, Conseiller auprès du secrétaire d'Etat

Secrétariat général aux affaires européennes

- M. Francesco Gaeta, secrétaire général adjoint
- Mme Christine Cabuzel-Duvallon, secteur numérique politique industrielle (ITEC), ajointe au chef de secteur
- M. Loic Agnès, chef du secteur ITEC

Direction générale des médias et des industries culturelles

- Mme Elizabeth Le Hot, sous-direction du développement de l'économie culturelle, sous-directrice
- Mme Victoire Citroën, bureau des affaires européennes internationales, cheffe de bureau
- Mme Laura Desille, bureau des affaires européennes internationales, chargée de mission
- Mme Joanna Chansel
- Mme Sophie Bouquet, secrétariat général, service des affaires juridiques et internationales, chargée de mission

Direction générale des entreprises

- M. Olivier Corolleur, sous-direction des communications électroniques et des postes, sous-directeur
- M. Jean-Pierre Labe, bureau de la réglementation des communications électroniques, chef de bureau
- Mme Mélanie Przyrowski, bureau de la réglementation des communications électroniques, chargée de mission

Direction générale de la concurrence, de la consommation et de la répression des fraudes

- Mme Joanna Ghorayeb, sous-direction des affaires juridiques, des politiques de la concurrence et de la consommation, sous-directrice
- M. Philippe Guillermin, bureau Politique de protection des consommateurs et loyauté, chef de bureau
- M. Hugo Bruel, bureau Politique de protection des consommateurs et loyauté, adjoint au chef de bureau

Autorité de régulation des communications électroniques et des postes (ARCEP)

- M. Zacharia Alahyane, Direction « Internet et Utilisateurs », directeur

- M. Olivier Delclos, Direction « Internet et Utilisateurs », unité opérateurs et obligations légales, chef d'unité
- Mme Jennifer Siroteau, Direction « Economie, marchés et numérique », unité analyse économique et intelligence numérique, cheffe d'unité
- M. Vincent Toubiana, Direction « Economie, marchés et numérique », unité analyse économique et intelligence numérique, chargé de mission
- Mme Annabel Gandar, Direction « Affaires juridiques », unité Infrastructures et réseaux ouverts, chargée de mission
- Mme Clara Hanot, Direction « Europe et international », unité Europe, chargée de mission

Commission Nationale de l'informatique et des libertés (CNIL)

- M. Jean Lessi, secrétaire général
- Mme Clémence Scottez, service du secteur économique, chef de service
- M. Brice Bastié, service des affaires économiques, juriste
- M. Heslot, service de l'expertise technologique, ingénieur

Conseil National du Numérique (CNN)

- M. Rand Hindi, membre du CNN, fondateur de Snips
- M. Charly Berthet, responsable juridique et des relations institutionnelles

Organisation professionnelles

Fédération e-commerce et vente à distance (fevad)

- M. Marc Lolivier, délégué général

Fédération nationale de la presse spécialisée (FNPS)

- M. Laurent Bérard-Quelin, président
- Mme Catherine Chagniot, directrice déléguée
- Mme Aurélie Petit, responsable juridique et économique

France digitale

- M Nicolas Brienne, directeur général

Groupement des éditeurs de contenus et de services en ligne (Geste)

- Mme Corinne Denis, Directrice du Numérique et du Développement des revenus, Lagardère Active, et Vice-Présidente du GESTE
- M. Emmanuel Parody, Associé et Directeur des rédactions, Mind Media, et Secrétaire Général du GESTE
- Maître Etienne Drouard, Président de la Commission Enjeux Réglementaires du GESTE
- M. Amélien Delahaie, Juriste au GESTE
- Mme Louise Durand, Responsable des Affaires Juridiques et Réglementaires du GESTE

Syndicat de la presse indépendante d'information en ligne (SPIIL)

- Mme Karen Autret, directrice
- M. David Legrand, membre du bureau

Syndicat de la presse quotidienne nationale (SPQN)

- M. Denis Bouchez, directeur
- M. Samir Ouachtati, responsable des affaires juridiques et sociales
- Mme Béatrice Lhopitallier, Groupe Les Echos, directrice data
- M. Samuel Profumo, lefigaro.fr, directeur data & CRM

Syndicat des régies internet (SRI)

- Mme Hélène Chartier, directrice générale

Tech'in France

- M. Loïc Rivière, délégué général
- Mme Alice Garza, chargée de mission affaires publiques

Union des annonceurs (UDA)

- M. Jean-Luc Chetrit, directeur général
- Mme Laureline Frossard, responsable juridique
- Mme Laura Boulet, directrice affaires publiques, juridiques & éthiques

Union des entreprises de conseil et achat média (UDECAM)

- Mme Françoise Chambre, déléguée générale

Union de la presse en région (UPREG)

- Mme Maud Grillard, directrice
- M. Bruno Ricard, traitement des questions publicitaires

Association

La Quadrature du Net

- M. Arthur Messaud, juriste

Entreprises

Criteo

- M. Guillaume Marcerou, senior counsel Global Privacy Product
- M. François Costa de Beauregard, directeur général adjoint France

Google

- Rita Balogh, Public Policy and Government Relations Manager, Bruxelles
- M. Olivier Esper, directeur des relations institutionnelles
- M. Thibault Guiroy, affaires publiques et relations institutionnelles
- Lanah Kammourieh Donnelly, Public Policy and Government Relations Manager, Londres

Lysios

- M. Jean-Luc Archambault, président

Next Radio TV

- Mme Stéphanie Corbière, responsable juridique groupe

Orange

- M. Pierre Petillault, directeur adjoint des affaires publiques
- Mme Sophie Poncin, Orange advertising, directrice régie
- Mme Luisa Rossi, direction de la réglementation
- Anne Derouin, Responsable du Département Publicité, Services, Portails web et mobile

Qwant

- M. Léonard Cox, vice-président Affaires Publiques et RSE
- M. Guillaume Champeau, directeur Ethique et Relations Publiques

SFR

- Mme Marie-Georges Boulay, directrice des affaires réglementaires, concurrence, contrats opérateurs et fréquences
- M. Marc Jossermoz, directeur business development big data
- Mme Estelle Chevalier, responsable affaires européennes

S4M

- M. Nicolas Rieul, vice-président stratégie EMEA et administrateur responsable de l'international de la Mobile Marketing Association France

TF1

- M. Antony Level, directeur des affaires règlementaires numériques groupe
- M. Pierre Renaldo, expert data
- M. Ribadeau-Dumas, directeur-adjoint marketing digital

Groupe Vivendi

- Mme Chantal Andriotti, Canal+, responsable juridique Concurrence, Marketing de l'Offre, Données personnelles, NTIC
- M. Clément Reix, Dailymotion, directeur de projet « Affaires Publiques »
- M. Christophe Roy, Canal+, directeur des affaires européennes
- Mme Marie Sellier, Vivendi, directrice des Affaires Publiques
- M. Arnaud Schmite, havas media, secrétaire général

Wavestone

- M. Gabriel Amirault, senior consultant
- Mme Mathilde Bouget, stagiaire de Toulouse Business School

Personnes qualifiées

- M. Claude Castellucia, INRIA, directeur de recherche
- Mme Maryline Laurent, professeur, Telecom SudParis
- M. Daniel le Metayer, INRIA, directeur de recherche
- M. Patrick Waelbroeck, professeur, Telecom ParisTech

Cap Digital a organisé pour la mission le 8 novembre une discussion-débat sur le projet de règlement e-privacy, à laquelle a pris part une trentaine de membres du pôle de compétitivité.

Annexe 3 : le fonctionnement de la publicité programmatique

Pour une campagne de publicité ciblée, l'annonceur cherche à définir un groupe de personnes susceptibles d'être intéressées par un produit ou un service. L'analyse est essentiellement probabiliste : il s'agit de prédire un score d'intérêt pour le produit ou le service, de la part de personnes pouvant appartenir à certains segments de différentes catégories de données[64] : segmentation sociodémographique (sexe, âges, ayant ou non des enfants, profils sociodémographiques), segmentation des intentions d'achat d'un bien ou service (inférées à partir d'un historique de navigation), segmentation des intérêts ou hobbies, possession de certains types de produits, … Il y a donc une définition de la cible (le profil des internautes susceptibles d'être intéressés) et, quand un internaute appelle une page, un calcul pour rattacher ou non cet internaute à cette cible, à partir des données disponibles sur son propre profil.

L'annonceur s'appuie sur une agence ou une équipe de marketing interne, qui va utiliser un terminal (siège) relié à un DSP (*demand side platform*) pour acheter des espaces sur des pages (impressions) appelées par des internautes qui correspondent au profil visé. Ces espaces sont commercialisés par des SSP (*suply side platforms*) via des *Adexchanges*. Ce circuit de vente des espaces est complété par un circuit de ventes des données (*data first party, second party ou third party*), et par un circuit qui permet de servir les annonces (*adservers*).

Dans le cas du reciblage (*retargeting*), c'est l'intérêt manifesté par l'internaute pour un produit ou un service qui conduit à le lui proposer à nouveau lors d'une navigation ultérieure.

Les méthodes qui conduisent à proposer une publicité à un internaute sont analogues à celles qui permettent de faire une recommandation : les données recueillies sur un internaute permettent de calculer des correspondances (*matching*) à partir d'autres données de transactions enregistrées. Lors de nombreux tests, ces méthodes se sont révélées plus performantes que les méthodes d'analyse contextuelle (prédiction des intérêts de l'internaute à partir de ce qu'il est en train de faire).

Pour l'internaute, les étapes sont les suivantes :

1. L'internaute accède à une page web. Une requête est générée pour servir une annonce qui apparaitra sur cette page. Cette requête est traitée avec des données sur l'internaute. Ces données peuvent être connues du site, ou ont été compilées par une *data management platform* sur la base de cookies (*data 3rd party*).
2. La requête est adressée au serveur d'annonce du site web (ad serveur du support), qui sert en priorité les affichages correspondant aux ventes en direct, correspondant à des contrats passés par l'éditeur (ou sa régie publicitaire) avec des annonceurs (ou leurs agences).
3. S'il n'y a pas de ventes en direct, ou si celles-ci passent par le canal « programmatique », la requête est transmise à un a*dexchange* via un SSP. Cet *adexchange* communique avec de nombreux serveurs (DSP) susceptibles d'être intéressés par le placement de l'annonce. L'*adexchange* peut :
    a. Placer des ventes directes, dites « premium » quand il s'agit des meilleurs espaces publicitaires, tels que les pages d'accueil. Pour l'annonceur, l'intérêt de passer par l'*adexchange* pour des contrats en direct est d'automatiser sa campagne d'achats.

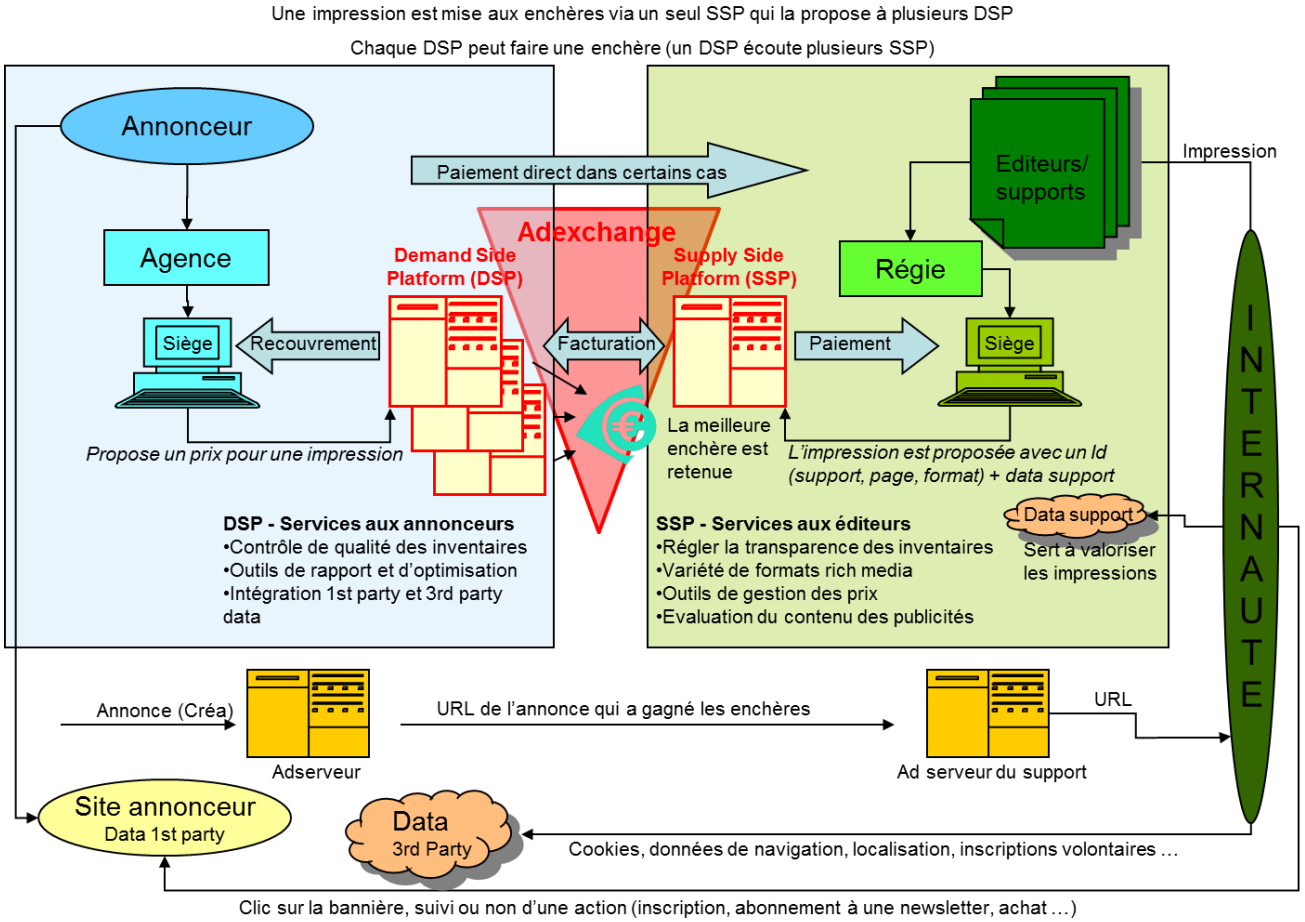
[64] Voir par exemple les catégories de données recensées dans le Eyeota H1 2017 Index Report

b. Servir de place de marché privée (seuls certains acheteurs sélectionnés par l'éditeur participent à la vente).
c. Servir de place de marché ouverte (Real Time Bidding, RTB). N'importe quel DMP connecté à la plateforme peut participer.

4. L'annonce est vendue, après mise aux enchères auprès de parties tierces (cas b. et c.).
5. L'enchère est remportée (en général par celui qui propose le prix le plus élevé, mais pour le prix de la 2ème offre). Ceux qui participent aux enchères peuvent le faire sur la base de données accompagnant la requête, mais aussi sur la base de données propres dont ils disposent (par exemple pour du reciblage / retargeting)).
6. L'annonce est servie à l'internaute.

L'attrait du canal programmatique tient à son efficacité technique et à sa souplesse. Ses limites viennent de la difficulté, d'une part, de contrôler la qualité des données, d'autre part, de mesurer la visibilité de l'annonce (temps d'affichage partiel ou complet, affichages générés par des machines, parfois frauduleux). En outre l'acheteur ne sait pas sur quel site il achète, il peut seulement paramétrer des listes de sites, blanches ou noires. De son côté, en RTB, l'éditeur peut seulement jouer sur un prix plancher et définir une liste d'annonceurs indésirables. Les achats directs ou via des ventes privées sont réputés offrir une meilleure garantie de visibilité que le RTB. Au sein du canal programmatique, la part prise par les ventes directes ou privées, qui se développent depuis 2010, est donc liée au souhait des annonceurs d'acheter des espaces de qualité et de mieux maîtriser la visibilité des annonces.

Vente d'une impression sur un Adexchange, place de marché



Annexe 4 : texte des articles 8,9 et 10 du projet de règlement e-privacy

Texte des articles 8,9 et 10 du projet de règlement e-privacy proposé par la Commission et amendements correspondants du projet de résolution législative du parlement européen adopté le 26 octobre 2017

Proposition de règlement
Article 8 - Titre

Texte proposé par la Commission	*Amendement*
Protection des informations ***stockées dans les*** équipements terminaux des utilisateurs ***finaux ou liées à ces équipements***	Protection des informations ***transmises aux*** équipements terminaux des utilisateurs ***et des informations qui y sont stockées, traitées ou collectées***

Proposition de règlement
Article 8

Texte proposé par la Commission	*Amendement*
1. L'utilisation des capacités de traitement et de stockage des équipements terminaux et la collecte d'informations provenant des équipements terminaux des utilisateurs finaux, y compris sur les logiciels et le matériel, sont interdites, sinon par l'utilisateur ***final*** concerné et pour les motifs suivants:	1. L'utilisation des capacités de traitement et de stockage des équipements terminaux et la collecte d'informations provenant des équipements terminaux des utilisateurs finaux, y compris sur les logiciels et le matériel, sont interdites, sinon par l'utilisateur concerné et pour les motifs suivants:
(y) cela est nécessaire à la seule fin d'assurer une communication électronique dans un réseau de communications électroniques; ou	(a) si cela est strictement nécessaire à la seule fin d'assurer une communication électronique dans un réseau de communications électroniques; ou
(z) si l'utilisateur ***final*** a donné son consentement; ou	b) si l'utilisateur a donné son consentement ***spécifique***; ou
(aa) si cela est nécessaire pour fournir un service de la société de l'information demandé par l'utilisateur ***final***; ou	c) si cela est ***strictement*** nécessaire***, sur un plan technique,*** pour fournir un service de la société de l'information ***spécifiquement*** demandé par l'utilisateur; ou
(bb) si cela est nécessaire pour mesurer ***des résultats d'audience sur le Web***, à condition que ce mesurage soit effectué par le fournisseur du service de la société de l'information ***demandé par l'utilisateur final.***	d) si cela est nécessaire***, sur un plan technique,*** pour mesurer ***la portée d'un service de la société de l'information demandé par l'utilisateur***, à condition que ce mesurage soit effectué par le fournisseur***, ou en son nom, ou par une agence indépendante d'analyse*** du ***web agissant dans l'intérêt public ou à des fins scientifiques; ces données sont agrégées et l'utilisateur dispose d'un***

droit d'objection; à condition qu'aucune donnée à caractère personnel ne soit accessible à une tierce partie et que le mesurage en question ne porte pas atteinte aux droits fondamentaux de l'utilisateur; lorsque la mesure d'audience est effectuée au nom d'un fournisseur de service de la société de l'information, les données collectées sont traitées uniquement pour ce fournisseur et sont maintenues séparées des données collectées dans le cadre de la mesure d'audience au nom d'autres fournisseurs; ou

d bis) si cela est nécessaire pour garantir la sécurité, la confidentialité, l'intégrité, la disponibilité et l'authenticité de l'équipement terminal de l'utilisateur final au moyen de mises à jour, pendant la durée nécessaire à cette fin, à condition:

i) que cela ne modifie en aucune façon la fonctionnalité de l'équipement matériel ou logiciel ou les paramètres de confidentialité choisis par l'utilisateur;

ii) que l'utilisateur soit informé à l'avance chaque fois qu'une mise à jour est en cours d'installation; et

iii) que l'utilisateur ait la possibilité de reporter ou de désactiver la fonction d'installation automatique de ces mises à jour.

d ter) dans le contexte des relations de travail, si cela est strictement nécessaire, sur un plan technique, pour l'exécution de la tâche d'un employé, lorsque:

i) l'employeur fournit l'équipement terminal et/ou est l'utilisateur;

ii) l'employé est l'utilisateur de cet équipement terminal; et

iii) cela ne sert pas accessoirement à surveiller l'employé.

1.bis Nul utilisateur ne peut se voir refuser l'accès à un service ou à une fonctionnalité de la société de l'information, payant ou non, au motif qu'il n'a pas consenti, comme le prévoit l'article 8, paragraphe 1, point b), à un traitement de ses données à caractère personnel ou à une utilisation des capacités de traitement ou de stockage de ses équipements terminaux non nécessaire à la fourniture du service ou de la fonctionnalité.

2. *La collecte* d'informations émises par l'équipement terminal pour permettre sa connexion à un autre dispositif ou à un équipement de réseau est interdite, sauf si:	**2. *Le traitement*** d'informations émises par l'équipement terminal pour permettre sa connexion à un autre dispositif ou à un équipement de réseau est interdite, sauf si:
(cc) elle est pratiquée exclusivement dans le but d'établir une connexion et pendant la durée nécessaire à cette fin; ou	*a) elle est pratiquée exclusivement dans le but d'établir une connexion, **demandée par l'utilisateur**, et pendant la durée nécessaire à cette **seule** fin; ou*
	a bis) l'utilisateur a été informé et a donné son consentement; ou
	a ter) les risques sont atténués.
(dd) un message clair et bien visible est affiché, indiquant les modalités et la finalité de la collecte et la personne qui en est responsable, fournissant les autres informations requises en vertu de l'article 13 du règlement (UE) 2016/679 lorsque la collecte porte sur des données à caractère personnel, et précisant les mesures éventuelles que peut prendre l'utilisateur final de l'équipement terminal pour réduire au minimum la collecte ou la faire cesser.	***Supprimé***
La collecte de ces informations est subordonnée à la mise en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, comme le prévoit l'article 32 du règlement (UE) 2016/679.	***Supprimé***
	2 bis. Aux fins du paragraphe 1, point d), et du paragraphe 2, point a ter), les contrôles suivants sont mis en œuvre pour atténuer les risques:
	a) la finalité de la collecte de données à partir de l'équipement terminal est limitée à un simple comptage statistique; et
	b) le traitement est limité dans le temps et dans l'espace, et dans la mesure strictement nécessaire à cet effet; et
	c) les données sont effacées ou anonymisées immédiatement dès lors que la finalité est remplie; et
	d) les utilisateurs disposent d'un droit d'objection effectif sans effet sur les fonctionnalités de l'équipement terminal;

	2 ter. Les informations visées au paragraphe 2, points a bis) et a ter), sont communiquées au moyen d'un message clair et bien visible qui indique, au moins, le détail des modalités de collecte des informations, la finalité du traitement et la personne qui en est responsable ainsi que les autres informations requises en vertu de l'article 13 du règlement (UE) 2016/679, lorsque des données à caractère personnel sont collectées. La collecte de ces informations est subordonnée à la mise en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, comme le prévoit l'article 32 du règlement (UE) 2016/679.
3. Les informations à fournir en application du paragraphe 2, **point b**), peuvent être associées à des icônes normalisées de manière à offrir une vue d'ensemble efficace de la collecte, qui soit facile à visualiser, à comprendre et à lire.	3. Les informations à fournir en application du paragraphe 2 **ter**, peuvent être associées à des icônes normalisées de manière à offrir une vue d'ensemble efficace de la collecte, qui soit facile à visualiser, à comprendre et à lire.

Article 9

Texte proposé par la Commission	*Amendement*
1. La définition et les conditions du consentement ***figurant à l'article 4, paragraphe 11, et à l'article 7 du*** règlement (UE) 2016/679***/UE*** s'appliquent.	1. La définition et les conditions du consentement ***établies par le*** règlement (UE) 2016/679 s'appliquent.
2. Sans préjudice du paragraphe 1, si cela est techniquement ***possible et*** réalisable, aux fins de l'article 8, paragraphe 1, le consentement peut être exprimé à l'aide des ***paramètres*** techniques ***appropriés d'une application logicielle permettant d'accéder*** à ***Internet***.	2. Sans préjudice du paragraphe 1, si cela est techniquement réalisable, aux fins de l'article 8, paragraphe 1, ***point b***), le consentement peut être exprimé ***ou révoqué*** à l'aide des **spécifications** techniques ***pour les services de communication électronique ou les services de la société de l'information qui permettent un consentement spécifique à des fins spécifiques et au regard de fournisseurs spécifiques activement sélectionnés par l'utilisateur dans chaque cas, conformément au paragraphe 1. Lorsque ces spécifications techniques sont utilisées par l'équipement terminal de l'utilisateur ou le logiciel installé sur ledit terminal, elles peuvent signaler le choix de l'utilisateur au regard des choix actifs précédemment effectués par celui-ci.***

	Ces signaux sont contraignants pour tout tiers et lui sont opposables.
3. Les utilisateurs ***finaux*** qui ont donné leur consentement au traitement de données de communications électroniques conformément à l'article 6, paragraphe 2, point c), ***et*** à l'article 6, paragraphe 3, points a) et b), ont la possibilité de retirer leur consentement à tout moment, comme prévu à l'article 7, paragraphe 3, du règlement (UE) 2016/679, ***et cette possibilité leur est rappelée tous les six mois*** tant que le traitement se poursuit.	3. Les utilisateurs qui ont donné leur consentement au traitement de données de communications électroniques conformément à l'article 6, paragraphe 2, point c), à l'article 6, paragraphe 3, points a) et b), ***à l'article 8, paragraphe 1, point b), et à l'article 8, paragraphe 2, point a bis),*** ont la possibilité de retirer leur consentement à tout moment, comme prévu à l'article 7, paragraphe 3, du règlement (UE) 2016/679, tant que le traitement se poursuit.
	3 bis. Tout traitement reposant sur un consentement ne doit pas avoir d'incidence négative sur les droits et les libertés des personnes dont les données à caractère personnel sont liées à la communication ou transmises par celle-ci, en particulier le droit à la protection de la vie privée et des données à caractère personnel.
Article 10	
Texte proposé par la Commission	
1. Les logiciels mis sur le marché qui permettent d'effectuer des communications électroiques, y compris la récupération et la présentation d'informations sur Internet***, offrent la possibilité d'empêcher les tiers de stocker des informations sur l'équipement terminal d'un utilisateur final ou de traiter des informations déjà stockées sur ledit terminal.***	1. Les logiciels mis sur le marché qui permettent d'effectuer des communications électroniques, y compris la récupération et la présentation d'informations sur Internet***:***
	a) sont dotés de paramètres de protection de la vie privée réglés par défaut de sorte à empêcher d'autres parties de transmettre des informations à l'équipement terminal d'un utilisateur ou d'y stocker des informations ainsi que de traiter des informations déjà stockées sur ledit terminal ou collectées sur celui-ci, sauf aux fins visées à l'article 8, paragraphe 1, points a), et c);
	b) au moment de l'installation, informent l'utilisateur et lui donnent la possibilité de modifier ou de confirmer les paramètres de confidentialité visés au point a) en requérant son approbation du paramétrage concerné, et lui donnent la possibilité d'empêcher d'autres parties de traiter des informations qui sont transmises à son équipement terminal, qui y sont stockées ou qui y sont collectées, aux fins prévues à l'article 8, paragraphe 1, points a), c), d) et d

bis);

c) offrent à l'utilisateur la possibilité d'exprimer son consentement explicite par l'intermédiaire des paramètres après l'installation du logiciel.

avant leur première utilisation, informent l'utilisateur des paramètres de confidentialité disponibles et précisent, dans le détail, les options de paramétrage disponibles en fonction du service de la société de l'information auquel l'utilisateur accède. Ces paramètres sont facilement accessibles pendant l'utilisation du logiciel et présentés de façon à permettre à l'utilisateur de prendre une décision en connaissance de cause.

1 bis. Aux fins:

a) du paragraphe 1, points a) et b);

b) de l'octroi ou du retrait du consentement, en application de l'article 9, paragraphe 2, du présent règlement, et

c) de l'opposition au traitement des données à caractère personnel en application de l'article 21, paragraphe 5, du règlement (UE) 2017/679;

les paramètres doivent déclencher, sur la base de spécifications techniques, un signal qui est envoyé aux autres parties afin de les informer des intentions de l'utilisateur en ce qui concerne l'octroi du consentement ou l'opposition au traitement. Ce signal est juridiquement valable et il contraignant pour tout tiers et lui est opposable.

1 ter. Conformément à l'article 9, paragraphe 2, ces logiciels garantissent qu'un service spécifique de la société de l'information permette à l'utilisateur de donner son consentement explicite. Un consentement explicite donné par un utilisateur en application de l'article 8, paragraphe 1, point b), prime sur les paramètres de confidentialité existants pour le service de la société de l'information concerné. Sans préjudice du paragraphe 1, lorsqu'une technologie spécifique a été autorisée par le comité de la protection des données aux fins visées à l'article 8, paragraphe 1, point b), le consentement peut

	être exprimé ou révoqué à tout moment, à la fois depuis l'équipement terminal et en suivant les procédures prévues par le service de la société de l'information concerné.
2. Au moment de l'installation, le logiciel informe l'utilisateur final des paramètres de confidentialité disponibles et, avant de continuer l'installation, lui impose d'en accepter un.	***Supprimé***
3. Dans le cas d'un logiciel qui était déjà installé à la date du ***25 mai 2018***, les exigences visées aux paragraphes 1 et ***2*** sont remplies au moment de la première mise à jour du logiciel, mais au plus tard ***le 25 août 2018***.	3. Dans le cas d'un logiciel qui était déjà installé à la date du ***[xx.xx.xxxx]***, les exigences visées aux paragraphes ***1,*** 1 ***bis*** et ***1 ter*** sont remplies au moment de la première mise à jour du logiciel, mais au plus tard ***six mois après [date d'entrée en vigueur du présent règlement]***.