Cahiers
#Costech

> Julien Rossi
> Florian Hémont

Droit, consentement et « dark patterns »

Étude de l'évolution des bandeaux cookies entre 2020 et 2021

> #Numéro 6
> Démocratie et numérique
> Working papers
> EPIN - Ecritures, Pratiques et Interactions Numériques (Costech-UTC)
> Design - > Libertés et droit

Citer cet article

Rossi, Julien., Florian Hémont. "Droit, consentement et « dark patterns ». Étude de l'évolution des bandeaux cookies entre 2020 et 2021", 3 avril 2023, *Cahiers Costech*, numéro 6.
DOI https://doi.org/10.34746/cahierscostech156 -
URL https://www.costech.utc.fr/CahiersCostech/spip.php?article156

Working paper rédigé dans le cadre du projet WebConsentement (Action Spécifique - Université Rennes 2), présentant des travaux de recherche en cours.

Résumé

Une majorité des sites web populaires dans l'Union européenne affichent aujourd'hui une interface de recueil du consentement à l'activation de cookies et au pistage de la navigation de leurs visiteurs lorsque ceux-ci s'y rendent pour la première fois. Cet affichage découle d'obligations légales, et notamment de l'article 5 paragraphe 3 de la directive européenne 2002/58/CE lu en combinaison avec le Règlement général de protection des données. La façon dont le droit de l'Union conceptualise le consentement au traitement de données à caractère personnel n'est toutefois pas la seule acception possible du terme « consentement », dont de nombreux travaux ont souligné une polysémie qui s'incarne dans la diversité du design des bandeaux cookies. Si, lors d'une étude réalisée sur les 90 bandeaux cookies identifiés sur les 99 noms de domaine les plus visités en France en 2020, tous incarnaient une conception traduisant l'adage « qui ne dit mot consent ». Nous avons observé en 2021 une diminution sensible de certains dark patterns qui conduisent les internautes à des comportements de consentement résigné, ainsi qu'une nette augmentation de la proportion de bandeaux cookies mettant en scène, par leurs textes et par les interactions proposées, un consentement opt-in qui traduit l'adage : « si c'est pas oui, c'est non ». Cette évolution est corrélée à des sanctions d'autorités de protection des données, mais aussi au passage à une nouvelle version du standard technique qui sous-tend le fonctionnement de la majorité des bandeaux cookies de notre corpus : le Transparency and Control Framework. Le présent article présente quelques résultats intermédiaires du projet WebConsentement de l'Université Rennes 2, et dessine des pistes de recherche pour la suite de ce projet.

Mots-clefs : vie privée, surveillance, design, dark patterns, droit, consentement

Auteur(s)

Julien Rossi est maître de conférences à l'Université Paris 8, chercheur au Centre d'études sur les médias, les technologies et l'internationalisation, chercheur associé au COSTECH à l'Université de technologie de Compiègne et au PREFICS à l'Université Rennes 2. Il coordonne le Groupe de travail sur la régulation et la gouvernance d'Internet du GDR Internet, IA et Société du CNRS. Ses travaux portent sur la production et l'usage de normes juridiques et techniques de protection de la vie privée et des données personnelles.

Florian Hémont est maître de conférences à l'Université Rennes 2, et chercheur au Pôle de Recherche Francophonies, Interculturel, Communication, Sociolinguistique (PREFICS). Sa recherche recherche s'intéresse aux médiations qui prennent place autour des Technologies Numériques d'Information - Communication.

Plan

Bandeaux cookies et Consent Management Platforms

Lorsqu'un internaute visite une page web, le site qu'il visite peut enregistrer des cookies[1] sur son terminal, via son navigateur. Les données contenues dans ces cookies pourront alors être lues par ce site lors de la prochaine visite. Cela peut servir à enregistrer les préférences linguistiques de l'utilisateur, ou les paramètres d'une session, mais cela peut aussi contribuer à exercer une surveillance sur la navigation d'un internaute, et ce particulièrement lorsque ces cookies sont enregistrés non pas par des first-parties (c'est-à-dire par le site que l'internaute sait qu'il visite) mais pas des third-parties, qui sont d'autres sites, contenant des ressources auxquelles le first-party visité par l'internaute fait appel (par exemple un bouton « like » d'un réseau social). D'autres techniques

existent pour parvenir à ce résultat et sont détaillées dans un article de Steven Engelhardt et Arvind Narayanan (Englehardt et Narayanan, 2016). La principale finalité de tels traitements est le profilage à des fins soit de personnalisation du contenu, soit de personnalisation de la publicité.

Selon Martin Degeling et al. (2019), environ 62 % des sites web populaires dans l'Union européenne étaient dotés, en 2019, d'un bandeau cookie prévenant l'utilisateur de la présence de ce type de technologie de pistage sur le site qu'il visite. Ce sont ces bandeaux qui nous intéresseront dans la présente étude.

Cristiana Santos, Nataliia Bielova et Célestin Matte définissent un bandeau cookie comme « un moyen de recueillir le consentement de l'utilisateur pour l'utilisation de cookies et éventuellement d'autres technologies d'applications web qui peuvent enregistrer des données ou exploiter les attributs du navigateur pour reconnaître le navigateur de l'utilisateur (selon la technique du *browser fingerprinting*)[2] » (Santos, Bielova et Matte, 2019, p. 3).

Il en existe une grande diversité. Le point commun de ces interfaces est qu'elles se présentent comme une réponse à des obligations juridiques, et proposent une forme d'information à destination de l'utilisateur sur la présence de cookies ou d'autres technologies de pistage sur la page qu'il visite. Ils offrent ensuite, généralement, des possibilités d'interaction qui permettent la performance[3] de son consentement à tout ou partie de ces cookies, de ces technologies de traçage et des finalités auxquels ils sont employés.

Certains bandeaux cookies sont générés par des logiciels appelés des Consent Management Platforms (CMPs), comme Didomi ou Cookiebot. Ces logiciels sont faits pour être installés sur un grand nombre de sites web. Ils proposent à ceux qui les déploient une gamme de paramètres, tout en participant à une standardisation des formes et des textes des bandeaux cookies rencontrés par les utilisateurs. Ces CMPs peuvent aussi gérer l'enregistrement du consentement de l'utilisateur et sa transmission aux third-parties publicitaires présents sur les sites où ils déployés.

Une grande partie des CMPs repose sur le standard Transparency and Control Framework (TCF) de l'Interactive Advertisement Bureau, une association regroupant les acteurs de l'industrie de la publicité

comportementale. Il définit un mode de communication entre l'internaute et l'ensemble de la chaîne de traitement de données personnelles permettant l'affichage de publicité personnalisée sur le site visité par celui-ci. Pour ce faire, il décrit notamment le format d'une chaîne de caractère qui encode un signal sur les finalités auxquelles un internaute consent par son interaction avec un bandeau cookie, et la façon dont cette chaîne de caractère est transmise à ces différents acteurs, leur permettant (en théorie) de démontrer leur conformité juridique (Santos et al., 2021).

Quel consentement incarnent les bandeaux cookies, et qui le détermine ?

Les travaux sur le sujet des bandeaux cookies en général et des CMPs en particulier, tendent à montrer un faible taux de conformité de ceux-ci aux règles de droit dont ils sont censés contribuer au respect.

Nous savons que le design des bandeaux cookies peut avoir une forte influence sur le comportement des internautes. Christine Utz et al. (2019) ont en effet montré que les taux de clics par des internautes sur le bouton d'un bandeau cookie permettant de signifier un consentement au pistage, par exemple à des fins de personnalisation de la publicité, variaient de 0,1 % à 50,8 % en fonction notamment de l'emplacement du bandeau, du bouton, et des options proposées. Cela montre l'influence du design sur le comportement des internautes, dont les travaux de Midas Nouwens et al. (2020) suggèrent qu'ils sont une large proportion à éprouver une forme de lassitude à l'égard des bandeaux cookies qui les conduit à cliquer sur les boutons d'acceptation pour gagner du temps et accéder au contenu.

Or, Christine Utz et al. (2019) estiment que 86 % des bandeaux étudiés dans leur corpus ne proposaient en guise de consentement qu'un bouton de confirmation sans possibilité d'exprimer un refus. Une étude de Célestin Matte, Nataliia Bielova et Cristiana Santos de 2020 montrait qu'environ 10 % des sites de leur échantillon enregistrait un consentement de l'internaute avant toute action de celui-ci. Selon Midas Nouwens et al. (Nouwens et al., 2020), seuls 11,8 % des 680 sites que leur script a pu étudier sur un corpus des 10 000 sites les plus populaires au Royaume-uni semblaient conformes aux obligations minimales en matière de consentement dans le droit de l'Union européenne de protection de la vie privée et des données à caractère personnel.

L'obligation de demander à un internaute qui visite un site web son consentement à l'inscription de cookies – nécessitant une opération de lecture/écriture – sur son terminal a été précisée par un amendement de 2009 à l'article 5 (3) de la directive 2002/58/CE, dite e-Privacy[4]. Ce consentement s'entend au sens défini par la directive 95/46/CE sur la protection des données[5], désormais remplacée par le Règlement général de protection des données (RGPD)[6]. Le fait qu'entre l'adoption des amendements à la directive e-Privacy de 2002 et les différentes études que nous venons de citer, une dizaine d'années se soient écoulées sans que la majorité des sites ne se soient mis en conformité, suggère une forme d'incapacité du droit et de ses institutions à faire appliquer des règles au fonctionnement d'Internet et du Web, notamment en vue de garantir l'effectivité du droit à la vie privée et de celui à la protection des données à caractère personnel.

Pourtant, Martin Degeling et al. (2019) ont montré que le pourcentage des sites populaires en Europe étudiés dans leur corpus et affichant un bandeau cookie était passé de 46,1 % à 62,1 % entre janvier et mai 2018, à l'approche de l'entrée en application du RGPD en mai 2018. Ce règlement prévoit, pour certaines catégories d'infractions, des sanctions pouvant aller jusqu'à 4 % du chiffre d'affaires mondial d'une entreprise, ou 20 millions d'euros, le chiffre le plus élevé étant retenu.

Dans le cadre du projet WebConsentement, financé par une action spécifique de l'Université Rennes 2, nous avons fait l'hypothèse qu'au-delà de questions bien présentes et bien étudiées de conformité et d'application du droit, ce qui se jouait dans le design des bandeaux cookies était aussi une bataille sémantique autour de la définition du consentement.

Le sens de ce mot n'a rien d'une évidence. Là où Marie-Anne Frison-Roche (1995) voit dans le consentement une soumission à la volonté d'autrui, l'article 4 du RGPD définit le consentement comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement. » Maxence Christelle (2014) et Geneviève Fraisse (2017) ont insisté dans leurs travaux sur cette polysémie du consentement, dont nous pouvons distinguer au moins ces deux formes opposées, l'une pouvant se résumer par l'adage « qui ne dit mot consent » (on parle aussi de consentement opt-out), et l'autre par : « si c'est pas oui,

c'est non » (qui est un consentement opt-in). Maxence Christelle (2014) et Nathalie Sarthou-Lajus rappellent aussi l'existence de l'acception héritée des stoïciens, selon lesquels l'ataraxie naît du fait que le « sage ne se laisse pas troubler par les événements car il sait accorder son jugement à l'ordre des choses et se résigner devant l'inéluctable » (Sarthou-Lajus, 2009, p. 779). Contrairement à ce que nous supposions avant de lire ces travaux, ainsi que ceux de Clément Cousin (2016) sur le consentement à l'acte médical, l'avènement du consentement libre et éclairé dans de nombreux domaine du droit est un phénomène récent, qui a pris de l'ampleur dans la seconde moitié du XX^{e} siècle, et qui n'est pas encore tout à fait stabilisé. Les controverses autour du design des bandeaux cookies, qui ont été portées jusqu'à des contentieux devant le Conseil d'État7 et la Cour de justice de l'Union européenne (CJUE)8, s'inscrivent dans ce cadre général d'évolution à la fois de la place occupée par le consentement dans la régulation des relations entre individus et entre l'individu et la société, et du sens attribué à ce mot.

Notre enquête se situe au croisement de deux démarches théoriques et méthodologiques. Dans un premier temps, nous nous intéressons à la façon dont les bandeaux cookies matérialisent des discours et des conceptions normatives sur le consentement, en nous inspirant de travaux en Sciences and Technology Studies (STS) et notamment des travaux théoriques de Peter-Paul Verbeek (2006). Cette analyse a reposé en large part sur une analyse techno-sémiotique du dispositif, qui emprunte notamment à la théorie des écrits d'écrans (Jeanneret et Souchier, 2005 ; Souchier, 1996). Nous analysons ensuite la façon dont ces discours et conceptions normatives sont matérialisées par les dispositifs étudiés en comparaison avec les obligations juridiques qui découlent de règles de droit positif, en mobilisant une méthode d'analyse juridique des dark patterns proposée par Colin Gray, Cristiana Santos, Nataliia Bielova, Michael Toth et Damian Clifford (Gray et al., 2021).

Ce document de travail a pour objectif principal de partager des résultats intermédiaires de travaux en cours dans le cadre du projet WebConsentement financé par l'Université Rennes 2, le Pôle de Recherche Francophonies, Interculturel, Communication, Sociolinguistique (PREFICS) et le Laboratoire Interdisciplinaire de Recherche en Innovations Sociétales (LiRIS). Il porte sur des données collectées entre 2020 et 2021 par Florian Hémont, Gaël Hénaff et Julien Rossi, et à l'analyse desquelles a également participé Gudrun Ledegen.

Déroulement de l'enquête

Plusieurs travaux ont étudié à l'aide de méthodes partiellement automatisées de larges corpus de bandeaux cookies. Ainsi, Midas Nouwens et al. (2020) ont récolté par scraping[9] des données de 680 sites à partir d'un corpus constitué des 10 000 sites les plus populaires au Royaume-Uni. Martin Degeling et al. (2019) ont annoté manuellement un corpus de plus de 6000 sites web, pour vérifier la présence ou non d'un bandeau, et classer celui-ci parmi sept catégories assez larges. Une limite de ce travail est que seuls les sites compatibles avec la méthodologie ont été retenus dans le corpus, et qu'il ne s'agit pas nécessairement de sites populaires, plus proches de l'expérience quotidienne.

En partant de l'hypothèse que la centaine (environ) de sites les plus visités concentrait l'essentiel du temps passé et de l'expérience d'un internaute sur le Web, mais aussi en raison de contraintes de moyens limités et de coût des listes commerciales des sites les plus populaires par pays, nous avons choisi de ne constituer notre corpus qu'à partir des 99 noms de domaine *pay-level*[10] les plus populaires en France en mai 2020, selon le classement opéré par SimilarWeb, dont la liste était gratuitement accessible. Nous avons visité ces sites en 2020, puis de nouveau en 2021. Nous avons collecté des captures d'écran et des enregistrements vidéos d'interactions avec ces sites, analysé les bandeaux cookies présents et leur conformité (ou non) avec le standard TCF de l'IAB, et collecté des données sur leur conception et sur les textes affichés sur ces bandeaux. Nous avons opéré manuellement, de façon à ne pas exclure de sites de notre corpus à cause d'une incompatibilité entre le script que nous aurions rédigé pour collecter des données de façon automatique et le site visité. En 2020, cette approche nous a permis de collecter des données sur 90 bandeaux cookies, contre 89 en 2021. Cette démarche nous a permis d'étudier de façon fine les discours sur le consentement portés par ces bandeaux ainsi que de consigner les éventuels dark patterns observés.

Les dark patterns sont définis par Harry Brignull comme des « ruses, utilisées sur des sites web et des applications qui vous font acheter ou vous inscrire à des choses que vous ne vouliez pas » (Brignull, n.d.). Colin Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt et Austin L. Toombs (2018) distinguent cinq catégories de dark patterns :

- l'insistance lourde (*nagging*), définie comme une « redirection de la fonctionnalité attendue qui persiste au-delà d'une ou plusieurs interactions » (Gray et al, 2018, p. 5),
- l'obstruction, définie comme le fait de « rendre un processus plus difficile que nécessaire dans le but de dissuader certaines actions » (Gray et al, 2018, p. 5),
- la duperie (sneaking), qui est une « tentative de cacher, déguiser, ou retarder l'affichage d'une information utile à l'utilisateur » (Gray et al, 2018, p. 5),
- l'interférence d'interface, qui est une « manipulation de l'interface utilisateur qui privilégie certaines actions plutôt que d'autres » (Gray et al, 2018, p. 5),
- l'action forcée, qui consiste à « exiger de l'utilisateur qu'il fasse une action pour accéder, ou continuer à accéder, à une certaine fonctionnalité » (Gray et al, 2018, p. 5).

Dans le cadre d'une réflexion qui est encore en cours et qui demande à s'interroger sur la façon dont l'intersection entre textes, formes graphiques et possibilités d'interaction constituent des interfaces génératrices de sens, nous avons assigné de façon provisoire plusieurs caractéristiques à chacune de ces catégories :

Type de *dark pattern*	**Nous avons classé dans chaque catégorie les bandeaux qui …**
Insistance lourde	… restaient visibles tant que l'utilisateur n'interagissait pas avec. … continuaient à demander un consentement alors que l'utilisateur avait déjà actionné le signe passeur destiné à refuser (nous entendons par signe passeur, au sens de Jeanneret et Souchier (1999), tout signe support d'un lien hypertexte, qu'il prenne ou non la forme d'un bouton).
Obstruction	… n'affichaient pas de boutons pour refuser tous les traceurs dès la première étape d'interaction, au moment d'arriver sur le site … n'affichaient pas de bouton permettant d'accéder à des paramètres avancés dès la première étape d'interaction, au moment d'arriver sur le site … ne présentait aucun bouton pour refuser tous les traceurs, même après une première interaction avec le bandeau pour accéder à des options en étape 2 … renvoyaient uniquement aux paramètres du navigateur ou à des tiers pour permette à un internaute d'exprimer un refus … ne permettaient pas aux internautes de retirer leur consentement une fois celui-ci exprimé … ne permettaient pas de lire la politique de confidentialité permettant de faire un choix éclairé avant d'avoir exprimé un consentement … (en 2021 uniquement) imposaient l'étape d'un *opt-out* aux traitements fondés sur l'intérêt légitime du responsable du traitement en plus d'un refus de consentement pour refuser tout pistage
Duperie	… affichaient, en première étape, lors du chargement du site, un texte annonçant que la poursuite de navigation valait consentement. … affichaient, en première étape, lors du chargement du site, un texte présentant le consentement comme étant la possibilité de s'opposer. … ne donnaient aucune forme d'information sur les finalités des cookies ou autres traceurs et traitements de données auxquels l'internaute était invité à consentir. … disparaissaient lorsque l'internaute naviguait sur le site, même sans qu'il ait interagi avec lui. … disparaissait suite à une action de défilement de la page visitée. … disparaissait suite à un clic sur la bannière, même lorsque ce clic ne se faisait pas sur un signe passeur signifiant une disparition du bandeau. … (en 2021) affichaient un texte, en première étape, entretenant une confusion entre les conditions générales d'utilisation et l'acceptation des traceurs. … (en 2021) présentait des cases précochées en première étape ou dans l'étape 2, de paramétrage.
Interférence d'interface	… lorsque le texte affiché par le bandeau au moment du chargement initial du site affirme que le consentement des visiteurs à l'activation de traceurs est nécessaire à sa survie économique. … lorsque le texte affiché par le bandeau au moment du chargement initial du site culpabilise l'internaute en faisant peser sur lui la responsabilité de la protection de sa vie privée. … lorsque le texte affiché par le bandeau au moment du chargement initial du site affirme que l'activation de traceurs sert à l'amélioration de l'expérience de l'utilisateur. … lorsqu'un design incitatif est choisi pour le bouton permettant de consentir à toutes les finalités de tous les traceurs. … lorsque la signification du bouton permettant de cacher le bandeau revêt un sens ambigu. … lorsque le signe passeur permettant de fermer le bandeau est une croix à la signification ambiguë (par exemple : lorsqu'il n'est pas clair si un clic sur cette croix exprime un accord ou un refus)
Action forcée	… lorsqu'il est impossible d'accéder au site sans consentir. … lorsque le refus d'exprimer un consentement redirige l'internaute vers une page spécifique, qui n'est pas celle qu'il souhaitait visiter. … (en 2021) lorsque le refus des traceurs est subordonné à un paiement.

Nous avons ainsi suivi les évolutions dans le design des bandeaux cookies et les messages véhiculés dans leur conception et les textes qu'ils portent, et analysé leurs caractéristiques au regard des règles de

droit régissant le consentement au traitement de données à caractère personnel et l'accès en lecture-écriture au terminal d'un internaute par un site.

Contexte juridique

Détermination du droit applicable

Le RGPD définit les « données à caractère personnel » comme « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » (art. 4 (1) RGPD).

Les données collectées à des fins de profilage pour l'affichage de publicité personnalisée, ou même les données collectées pour identifier de façon unique chaque visiteur et générer des statistiques de visites, sont des données à caractère personnel même si elles n'identifient pas de façon directe les personnes concernées. Le simple fait de permettre de distinguer une personne d'une autre à partir de ses données suffit à faire entrer une donnée dans le champ des données à caractère personnel (Zuiderveen Borgesius 2016).

À son article 5, le RGPD définit un certain nombre de principes à respecter lors du traitement de données à caractère personnel. Le principe de licéité est l'un d'entre eux. L'un des critères permettant de respecter ce principe de licéité est celui du consentement de la personne concernée (art. 6 (1) (a) du RGPD). Si l'emploi de cookies ou d'autres techniques de stockage d'un identifiant unique sur le terminal de l'utilisateur n'est pas la seule façon pour un serveur distant de tracer les comportements des internautes, il s'agit encore d'une technique fortement répandue. Or, l'article 5 (3) de la directive e-Privacy de 2002, telle qu'amendée en 2009, dispose :

> « Les États membres garantissent que **le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement**. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur. »

Cette règle est transposée en droit français à l'article 82 de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le consentement en droit des données personnelles

Dans son arrêt du 1er octobre 2019, la Cour de justice de l'Union européenne a indiqué que cette notion d'« accord » était synonyme de « consentement » au sens de la directive 95/46/CE puis, depuis son entrée en application en mai 2018, du RGPD :

> « Au regard des éléments qui précèdent, le consentement visé à l'article 2, sous f), et à l'article 5, paragraphe 3, de la directive 2002/58, lus conjointement avec l'article 2, sous h), de la directive 95/46, n'est dès lors pas valablement donné lorsque le stockage d'informations ou l'accès à des informations déjà stockées dans l'équipement terminal de l'utilisateur d'un site Internet est autorisé au moyen d'une case cochée par défaut par le fournisseur du service, que l'utilisateur devrait décocher pour refuser de donner son consentement11. »

Cette jurisprudence a été confirmée dans un arrêt du 11 novembre 2020 dans un litige opposant la société Orange Roumanie à l'autorité roumaine de protection des données12.

Enfin, les cookies peuvent aussi être utilisés à des fins d'analyse statistique et de mesure d'audience. Cette dernière peut aussi se faire sans cookies. Dans ce cas-là, l'emploi de l'intérêt légitime, qui offre un mécanisme d'opt-out mais n'impose pas de consentement opt-in, semble plus cohérent avec le droit en vigueur. C'est en tout cas la position de la CNIL, qui rappelle toutefois que le recours à l'intérêt légitime pour la collecte de statistiques de mesures d'audiences agrégées doit

s'accompagner de mesures strictes, notamment pour garantir l'anonymisation rapide des données traitées13. Toutefois, certains logiciels de mesure d'audience, comme Google Analytics, ne servent pas seulement à générer des statistiques agrégées, mais jouent aussi un rôle dans la collecte de données à des fins de profilage publicitaire. C'est ainsi que l'installation de cookies Google Analytics sur les terminaux d'internautes visitant le site web de la chaîne Carrefour sans leurs consentements préalables a été condamné par une sanction de la CNIL du 18 novembre 2020 :

> « S'agissant de ces trois cookies, dits Google Analytics, la formation restreinte souligne qu'il ne fait pas débat que les données collectées par ces cookies peuvent être recoupées avec des données issues d'autres traitements pour poursuivre des finalités différentes que celles limitativement prévues par l'article 82 de la loi informatique et libertés, notamment pour mener à bien de la publicité personnalisée.
> Ces cookies n'ont pas pour finalité exclusive de permettre ou de faciliter la communication par voie électronique et ne sont pas strictement nécessaires à la fourniture du service. Leur dépôt aurait donc dû obliger la société à recueillir préalablement le consentement des utilisateurs. » (pts. 176 et 177 de la décision)

Cela laisse augurer – en tout cas selon la doctrine de la CNIL – qu'il soit possible dans certains cas de collecter des données de mesure d'audience sans le consentement *opt-in* de la personne concernée, sur la base de l'intérêt légitime du responsable du traitement. Mais cette option n'est pas nécessairement valable dès lors que le site web utilise une solution logicielle qui traite des données à d'autres fins que simplement la génération de statistiques agrégées anonymes.

Tous ces éléments nous ont amenés à conclure que, sauf rares exceptions à examiner au cas-par-cas dans des analyses détaillées, le consentement de la personne concernée est requis pour les finalités pour lesquelles les bandeaux cookies sont déployés.

Le consentement est défini dans le RGPD comme étant :

> « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement » (art. 4 (11) du RGPD).

La proposition de la Commission européenne, en 2012, définissait le « consentement » comme étant « explicite » (cf. document 2012-011 (COD) de la Commission européenne). Sous la pression des groupes d'intérêt industriels, cette proposition a été rejetée. Seul le consentement au traitement de certaines catégories de données sensibles définies à l'article 9 du RGPD est décrit avec la précision additionnelle qu'il doit être « explicite ». Cela n'a cependant qu'une incidence faible sur le fait que, contrairement à ce que réclamaient certains lobbies, le consentement « tacite » n'existe pas dans le RGPD. En d'autres termes, la conception du consentement que le droit consacre en matière de traitement de données à caractère personnel correspond à l'adage « si c'est pas oui, c'est non », et non à : « qui ne dit mot consent. »

Combiné à la lecture de l'article 25 énonçant un principe dit de vie privée par défaut (Privacy by Default), il en résulte que le consentement doit être un acte positif clair, une « manifestation de volonté ». La CJUE a donc jugé qu'une case pré-cochée par défaut ne pouvait pas constituer une méthode valide de recueil du consentement, car cela introduit un biais dans la manifestation de la volonté libre de la personne concernée14.

Le consentement doit en outre être spécifique, libre, et éclairé.

Le design et le droit

Tous ces éléments doivent donc se traduire dans le dispositif technique de recueil du consentement en ligne.

Concrètement, cela signifie que toute forme de dark pattern visant à biaiser le comportement de l'internaute (Waldman, 2020) est à proscrire. Ainsi, refuser les cookies (et autres technologies de pistages – mais nous allons parfois parler de « cookies » par simplicité d'écriture) doit être aussi facile que les accepter, comme l'a rappelé le Conseil d'État sans sa décision du 19 juin 202015. Il faut pouvoir exprimer sa volonté après avoir eu accès aux informations nécessaires pour faire un choix éclairé. Ces informations doivent être présentées de façon claire et lisible. L'article 7 du RGPD donne des précisions sur la notion de « liberté de choix » : il n'y a pas de consentement valable lorsqu'il y a une relation de pouvoir en défaveur de la personne concernée. Ainsi, un.e employé.e ne peut valablement consentir à un traitement de données le/la concernant par un employeur.

Un certain nombre questions juridiques restent aujourd'hui partiellement en suspens. Il s'agit notamment du cas où le pistage des internautes se déroule sans accès en lecture-écriture à son terminal, et du cas des « cookie walls ».

Le consentement et l'intérêt légitime du responsable du traitement

Nous avons vu qu'avec l'article 5 (3) de la directive e-Privacy, les responsables du traitement qui traitent les données à caractère personnel des internautes à des fins de publicité ciblée doivent recueillir ce consentement auprès des personnes concernées par le traitement. Ils ne peuvent s'appuyer sur le motif de leur intérêt légitime (art. 6 (1) (f) du RGPD).

Déjà au temps de la directive 95/46/CE, le G29 estimait que « les responsables du traitement pourraient invoquer l'article 7, point f), pour surveiller indûment les activités en ligne ou hors ligne de leurs clients, pour compiler d'importants volumes de données à leur propos en provenance de différentes sources, collectées à l'origine dans d'autres contextes et à des fins différentes, et pour créer – mais aussi, par exemple, échanger en passant par des courtiers en informations – des profils complexes concernant la personnalité et les préférences des clients, sans les en informer ni mettre à leur disposition un mécanisme fonctionnel permettant d'exprimer leur opposition, pour ne rien dire de leur consentement éclairé. Une telle activité de profilage risque de constituer une violation grave de la vie privée du client et, dans ce cas, l'intérêt et les droits de la personne concernée prévaudraient sur l'intérêt poursuivi par le responsable du traitement » (Groupe de travail de l'Article 29 2014, 29). Le G29 admettait certes que dans certains cas, un simple mécanisme d'opposition pouvait permettre au responsable du traitement de se fonder sur son intérêt légitime pour collecter des données à des fins de publicité, mais à condition que cette publicité ne soit pas personnalisée sur la base d'un profilage (Groupe de travail de l'Article 29, 2014, 35-36 ; 52 – 53).

Le considérant 47 du RGPD indique que « le traitement de données à caractère personnel à des fins de prospection peut être considéré comme étant réalisé pour répondre à un intérêt légitime. » Il est en outre indiqué, au considérant 70, que « lorsque des données à caractère personnel sont traitées à des fins de prospection, la personne concernée devrait avoir le droit, à tout moment et sans frais, de s'opposer à ce

traitement, y compris le profilage dans la mesure où il est lié à une telle prospection, qu'il s'agisse d'un traitement initial ou ultérieur. Ce droit devrait être explicitement porté à l'attention de la personne concernée et présenté clairement et séparément de toute autre information. »

Toute la question est de savoir dans quelle mesure la publicité personnalisée peut être considérée comme un traitement à des fins de « prospection ». Quoi qu'il en soit, une analyse fine des dispositions du RGPD combinée à la lecture d'autres règles de droit permettent à certains de conclure que les cas dans lesquels la collecte de données à des fins de publicité ciblée, fondée sur un profilage, peuvent se fonder sur le seul intérêt légitime du responsable du traitement sont rares. Le responsable du traitement doit en effet (entre autres) apporter la preuve qu'il ne collecte aucune donnée sensible (sur la santé, les opinions politiques, la sexualité …) protégée à l'article 9 du règlement, et qu'il est techniquement impossible de parvenir à réaliser son intérêt légitime sans employer de technique moins intrusive. Comme l'a noté à juste titre Frederik Zuiderveen Borgesius dans un article de 2015, il existe des systèmes qui permettent d'afficher de la publicité personnalisée sans faire sortir ses données personnelles de l'ordinateur de l'internaute (Zuiderveen Borgesius 2015 ; Toubiana et al. 2010).

Un autre argument à ajouter est qu'il y a lieu de tenir compte, dans l'interprétation du droit de l'Union européenne, des circonstances de son élaboration et de sa genèse, mais aussi de ses objectifs16. Or, les différents travaux préparatoires disponibles tendent à montrer que l'intention du législateur européen était notamment de renforcer les droits des personnes concernées en augmentant les garanties apportées au recueil du consentement et en réglementant la publicité comportementale en ligne. La Charte des droits fondamentaux de l'Union européenne, qui proclame un droit à la protection des données à caractère personnel à l'article 8, consacre également le consentement comme le fondement de droit commun de tout traitement de données à caractère personnel. Permettre à des tiers de collecter des données sur les internautes qui visitent une page web, comme cela se fait dans l'industrie de la publicité comportementale en ligne (Englehardt et Narayanan, 2016 ; Olejnik et Castelluccia, 2014) en contournant l'obligation de recueil de consentement posée par la directive e-Privacy (par l'emploi de techniques ne reposant pas sur des cookies ou d'autres formes d'écritures sur le terminal de l'utilisateur), est donc incohérent avec les objectifs poursuivis par la législation en vigueur. À notre

connaissance, cette question n'a pas encore fait l'objet d'un jugement, et nous ne faisons ici que proposer notre propre interprétation, mais, récemment, le Comité européen de protection des données a semblé prendre position (prudemment) contre les interfaces de bandeaux cookies qui prétendent recourir à l'intérêt légitime pour la publicité ciblée, y compris lorsqu'un tel traitement ne fait pas appel à des cookies (EDPB, 2023, p. 7).

L'incertitude sur les « *cookie walls* »

Une autre incertitude concerne les « cookie walls », ou « murs de cookies » en français. Ce terme désigne la subordination de l'accès à un site à l'acceptation des traceurs et traitements de données à caractère personnel proposés à l'internaute lors de sa première visite sur le site, généralement à l'aide d'un bandeau. En 2013, sur le fondement de l'ancienne directive, le G29 avait estimé qu'« en général, l'utilisateur devrait conserver la faculté de poursuivre sa navigation sur un site sans recevoir de cookies[17] » (G29, 2013, p. 5). Dans une déclaration du 25 mai 2018, le Comité européen de protection des données, succédant au G29, durcissait sa position au moment de l'entrée en application du RGPD, en affirmant :

> « Il convient de noter que le consentement qui doit être obtenu en vertu de la proposition de règlement ePrivacy a la même définition que dans le RGPD. En particulier, la nécessité d'obtenir le consentement libre des utilisateurs empêchera les fournisseurs de services de mettre en place des « cookie wall », c'est à dire de priver d'accès à leur site les utilisateurs n'acceptant pas les cookies et autres traceurs ; l'obligation d'obtenir le consentement spécifique de ces derniers créera des conditions de concurrence uniformes et équitables pour les fournisseurs, que l'utilisateur soit connecté ou non. » (CEPD, 2018, p. 3)

Dans sa délibération du 4 juillet 2019[18], la CNIL s'était appuyé sur cet avis pour affirmer que, selon elle « la pratique qui consiste à bloquer l'accès à un site web ou à une application mobile pour qui ne consent pas à être suivi (« cookie walls ») n'est pas conforme au RGPD » (art. 2 de la délibération de la CNIL du 4 juillet 2019).

Le Conseil d'État a estimé que cette recommandation était entachée d'illégalité par une décision du 19 juin 2020. Cet arrêt a souvent été présenté comme un aval donné par les juges du Palais Royal à tous les

cookie walls. Mais ce n'est pas le cas, et ce pour deux raisons. D'une part, comme le rappelle un communiqué de presse du Comité européen de protection des données du 19 novembre 2020, le Conseil d'État s'est borné à dire que la CNIL ne pouvait, sur la seule base de la directive e-Privacy et du RGPD, énoncer une interdiction générale des cookie walls. Il convient, selon cette juridiction, de vérifier au cas par cas si jamais l'impossibilité d'accéder au site constitue ou non un « inconvénient majeur »19. D'autre part, la CJUE peut toujours revenir sur cette interprétation du juge français, et il est probable qu'elle soit amenée à l'avenir à se prononcer.

Des propositions législatives étaient en cours de négociation au moment de la rédaction de ce papier en 2022, notamment des amendements à la proposition de Digital Services Act adoptés par le Parlement européen20, applicables seulement aux plateformes et pas à tous les sites web, et des dispositions de la proposition de réforme de l'actuelle directive e-Privacy par un nouveau règlement. Ces dernières prévoient, dans la version initiale de la Commission, la possibilité de se passer du consentement pour l'installation de cookies nécessaires à la productions de statistiques d'audiences21, l'obligation de demander le consentement y compris pour le pistage *stateless*22 (qui ne laisse pas d'enregistrement sur le terminal de l'internaute), mais aussi, selon des amendements proposés par un rapport de la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, une interdiction des *cookie walls*23.

Enfin, à côté des dispositions juridiques que nous venons de détailler, il existe des standards techniques dont l'objectif est de faciliter l'expression des préférences des internautes en matière de vie privée. Parmi ceux-ci, la Commission européenne comme le Parlement ont soutenu, par l'intermédiaire de la proposition de règlement e-Privacy, et de son article 9 en particulier, le projet de standard Do Not Track (DNT) que le World Wide Web Consortium (W3C), l'organisme de standardisation du Web, a finalement abandonné en 2019, faute de consensus sur son implémentation (Rossi, 2021). D'autres projets ont vu le jour, comme Global Privacy Control, soutenu entre autres par le navigateur Brave24, et l'Advanced Data Protection Control25, soutenue notamment par NOYB, l'association de Max Schrems, un juriste militant ayant fait invalider à deux reprises un accord de libre-échange de données personnelles entre l'Union européenne et les États-Unis d'Amérique. Il n'est toutefois pas certain que la proposition visant à obliger les sites web à respecter le signal de préférence envoyé depuis le

terminal de l'utilisateur selon l'un de ces standards soit retenue, car le Conseil de l'Union européenne, qui réunit les ministres des États membres, s'y oppose et demande la suppression de l'article 9 de la proposition initiale[26].

Cette longue exploration des règles applicables au recueil du consentement à l'installation de traceurs et au traitement de données à caractère personnel sur le Web, nous amène à conclure que s'il existe quelques points d'incertitude sur la possibilité de se passer du consentement lorsque le pistage d'un internaute ne requiert pas l'accès à son ordinateur en lecture ou en écriture, sur la légalité des cookie walls, et sur le rapport entre les règles de droit et les différents standards techniques qui visent à contribuer à la protection de la vie privée des internautes, le droit actuel impose dans tous les cas le recueil du consentement pour l'installation de cookies sur le terminal d'un internaute. Ce consentement est défini par le RGPD comme étant une manifestation de la volonté libre et éclairée de l'internaute, ce qui s'oppose nettement à une acception du consentement défini en référence à l'adage selon lequel « qui ne dit mot consent. » Les interfaces qui recueillent le consentement des internautes doivent s'assurer de l'absence d'ambiguïté quant au sens de l'interaction avec celle-ci. Plusieurs décisions de justice ont en effet souligné l'importance qu'aucun dark pattern ne vienne interférer avec la volonté de l'internaute. En d'autres termes : refuser les cookies doit être aussi facile que de les accepter.

Le marché des Consent Management Platforms (CMP) en France

En 2020, nous avons repéré 52 bandeaux générés par des outils tiers dédiés à la gestion du consentement, dont l'outil AdChoices, un programme d'auto-régulation du secteur de la publicité en ligne, sur un corpus de 90 sites web. Il ne prend pas l'apparence d'un bandeau cookie classique, mais d'une icône présente sur le site. En 2021, AdChoices était présent aux côtés d'un autre bandeau sur le site sur lequel nous l'avons repéré. Pour faciliter les comparaisons entre 2020 et 2021, nous l'avons donc sorti de notre définition des CMPs.

Il y avait donc 51 bandeaux ayant recours à une CMP en 2020, soit environ 57 % des sites étudiés disposant d'un bandeau, et 64 sur 89 en 2021, soit près de 72 % de notre corpus. Nous avons considéré comme étant une CMP tout bandeau généré par un script identifié utilisé par

plusieurs sites. Cette définition peut se discuter, dans la mesure où certains scripts ne sont que des morceaux de codes partagés par des développeurs sur des sites comme Github ou Stackoverflow. Mais nous avons fait le choix de distinguer les bandeaux cookies rédigés par les auteurs d'un site eux-mêmes, de ceux qui sont générés par du code fourni par un tiers, quel que soit ce code et quel qu'en soit son degré de sophistication.

Si la part des CMPs (au sens large de notre définition) a donc nettement augmenté, tous ne sont pas compatibles avec le standard technique édicté par l'Interactive Advertisement Bureau (IAB) : le TCF. Pour contrôler la conformité d'un bandeau utilisant une CMP au standard TCF, nous avons procédé selon trois méthodes différentes :

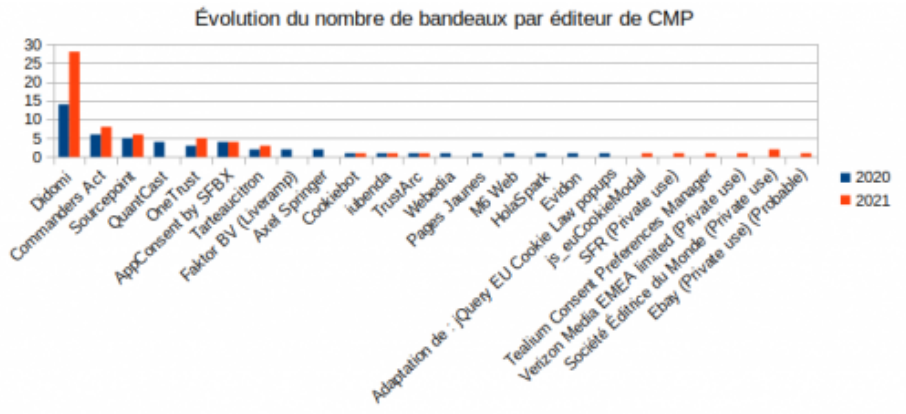
- un bandeau pouvait être comptabilisé comme conforme au TCF 1.1. s'il était détecté par l'extension de navigateur Cookie Glasses de Célestin Matte[27] ou à la version 2.0 s'il était détecté par notre propre extension de navigateur, construite à partir du code source de la précédente[28], et qui détectait la présence, conforme aux spécifications du TCF 2.0[29], d'un *iframe* « __tcfapiLocator » dans le code HTML du site[30] ;
- un bandeau pouvait être généré par une CMP conforme au TCF selon la liste des fournisseurs agréés par l'IAB[31] sans qu'il soit détecté par nos plug-ins, cette mesure ne tenant pas compte de la possibilité offerte par certains CMP, comme Didomi, de désactiver le signal TCF.

	Compatibilité TCF détectée par le plug-in	**CMPs présents sur la liste des fournisseurs agréés de l'IAB en 2021**
2020	28 (± 55 % des bandeaux générés par CMP)	*41 (environ)* (± 80 % des bandeaux générés par CMP) Ce chiffre est imprécis car au moment où nous avons consulté la liste des fournisseurs de CMP agréés par l'IAB, celle-ci correspondait déjà à la liste des CMP compatibles avec la version 2 du TCF. Or, certains fournisseurs de logiciels conformes à la version 1.1. du TCF n'ont pas produit de mise à jour. C'est le cas par exemple de M6Web et de Webedia. Si nous combinons la liste des CMP compatibles TCF détectés par le plug-in, avec celles dont le fournisseur était recensé parmi ceux dont les logiciels sont compatibles TCF au moment où nous avons consulté la liste, cela amène à un total de 47 bandeaux générés par une CMP dans notre corpus.
2021	39 (61 % des des bandeaux générés par CMP)	59 (± 92 % des bandeaux générés par CMP)

Une nette majorité des bandeaux est générée par des CMP, c'est-à-dire des logiciels dont l'auteur n'est pas le même que celui du site, sont donc conçus de façon conforme au TCF, qui est un standard technique édité

par l'Interactive Advertisement Bureau Europe (IAB Europe), une association qui regroupe les acteurs de l'industrie de la publicité en ligne en Europe. Fortement critiqué, y compris par l'Autorité de protection des données de Belgique[32], ce standard est le premier à être largement déployé et utilisé par un grand nombre d'acteurs économiques du web.

17 sites qui disposaient d'une CMP en ont changé entre 2020 et 2021. Voici l'évolution des parts de marché pour chaque acteur :



En 2020 : des sites unanimement non-conformes tournés vers un consentement résigné

Cristiana Santos, Nataliia Bielova et Célestin Matte (2019) proposent un tableau finement détaillé de 17 critères opérationnels permettant de juger de la conformité d'un bandeau cookie. Certains de ces critères exigent une évaluation approfondie au cas-par-cas. Par exemple, déterminer si un consentement est donné de façon « libre » nécessite un examen de la relation entre la personne concernée et l'opérateur du site web. L'évaluation de la validité du contenu des notices d'information mises à disposition des visiteurs du site est également délicate. Est-elle claire, complète ? Est-elle loyale et transparente ? Décrit-elle bien tous les éléments de pistage, visibles et invisibles, contenus sur la page ?

Pour des raisons évidentes de faisabilité, nous n'avons pas passé chaque site web visité au crible des 17 critères exhaustifs établis par Santos, Bielova et Matte. Nous ne sommes pas les seuls à avoir fait ce choix. Ainsi, Nouwens et al. (2020) (Nouwens et al., 2020) définissent trois critères de « conformité minimale » :

- Le fait que le consentement doive être explicite (opt-in) ;

- Le fait que refuser doit être aussi facile qu'accepter ;
- Le fait qu'il ne doive pas y avoir de case précochée dans l'interface.

Nous nous sommes focalisés sur l'expérience de l'utilisateur dans son interaction avec le bandeau. Nous n'avons donc par exemple pas vérifié si l'écriture de cookies (ou toute autre forme de pistage) attendait que nous ayons exprimé un consentement avant de s'enclencher. Par contre, nous avons tenu compte des différentes formes qui sont proposées à l'utilisateur : contenu des bandeaux cookies, formes des signes passeurs, et des formes d'interactions du dispositif de recueil du consentement pour évaluer leur présomption de conformité.

Pour notre étude, nous nous sommes basés sur les critères suivants, visibles dans l'interface, pour évaluer ce que nous avons appelé la *présomption de conformité* :

- Le consentement doit être *opt-in*, donc :
    - Le texte contenu dans le bandeau cookie ne doit pas évoquer la possibilité de recueillir un consentement tacite, par exemple par la poursuite de la navigation ;
    - Ce texte ne doit pas contenir de formulation tendant à faire passer le consentement aux cookies (et autres technologies assimilées) comme valable dès lors que la personne ne s'oppose pas au traitement. En d'autres termes, le bandeau ne doit pas faire exiger d'action d'*opt-out* pour refuser les cookies, mais au contraire être fondé sur une logique d'*opt-in* ;
- Le consentement doit être *informé*, donc :
    - Le texte du bandeau doit contenir une information minimale sur les finalités auxquelles l'utilisateur consent. Nous n'avons pas évalué la pertinence ou la qualité de ces informations, mais leur simple présence ou absence dès le premier stade de l'interaction avec le bandeau ;
    - Nous avons vérifié s'il était possible d'aller lire la politique de confidentialité complète du site web sur sa page dédiée sans avoir l'impression, en tant que visiteur, que le dispositif de consentement s'enclenche (disparition du bandeau cookie, ou message indiquant que nous avons consenti) ;
- Le consentement doit être *univoque* :
    - Le refus doit être aussi simple que l'acceptation. Pour que cela soit le cas, nous avons estimé que :
        - soit le bandeau présentait un bouton « refuser tout » dès la première étape d'interaction ;
        - soit le bandeau permettait un paramétrage facile des finalités pour lesquelles le visiteur donne son consentement dès la première étape.
    - Le fait de faire défiler la page (*scrolling*) ne doit pas enclencher le recueil du consentement ;
    - Le fait de cliquer sur la bannière, ailleurs que sur un bouton « j'accepte » ou assimilé, ne doit pas enclencher le recueil du consentement ;

En 2020, aucun des bandeaux de notre corpus ne répondait à ces critères. Il n'y avait alors qu'un seul site proposant un bouton « tout refuser » dès le chargement de la page, en première étape d'interaction.

En 2021 : le consentement *opt-in* devient majoritaire…

Entre nos première et seconde collectes de données, en 2020 et 2021, nous avons observé de nombreux changements. Ce changement se traduit notamment par le fait que désormais, 54 bandeaux sur 89 (soit près de 61 %), étaient désormais conformes aux critères présentés précédemment. Cette évolution s'est accompagnée d'une quasi-disparition des textes portant un discours selon lequel le consentement peut être tacite et exprimé par le simple fait de poursuivre sa navigation sur un site, comme par exemple dans le bandeau ci-dessous :

Bandeau du site caf.fr. Capture d'écran réalisée le 29 mai 2020.

En 2020, ces discours étaient présents sur 63 % des bandeaux, contre à peine un peu moins de 8 % en 2021.

L'exemple du bandeau ci-dessus est caractéristique d'un discours et d'un design qui mettent en scène une interaction de « consentement » où celui-ci est défini non pas comme une absence de refus, et encore moins comme une manifestation d'une volonté libre mais, conformément à la vision qu'en avaient les stoïciens antiques, c'est-à-dire telle une forme de soumission éclairée à la volonté d'autrui et, le cas échéant, divine. La seule possibilité d'action dans ce bandeau est l'énonciation d'un accord (par le bouton « OK ») ou l'action d'« en savoir plus » qui renvoyait, au moment de notre enquête, sur une politique de confidentialité statique au format PDF, sans possibilité de refus.

D'autres bandeaux, très nombreux en 2020 et moins en 2021, mettaient en scène un consentement tacite, mais pas totalement impuissant. Un discours sur la poursuite de la navigation valant accord pouvait être accompagné de la possibilité de refuser les traceurs, généralement au prix d'un nombre d'interactions avec le bandeau plus grand que dans l'hypothèse d'un accord. En 2020, 58 bandeaux, bien que ne présentant aucun bouton pour tout refuser dès la première étape, disposaient d'un bouton permettant d'accéder, en seconde étape, à une interface de

paramétrage comportant un bouton « tout refuser », comme dans l'exemple ci-dessous :

Étape 1 du bandeau cookie de purepeople.fr (logo flouté) le 1er juin 2020, avec un bouton vers « plus d'options »

Étape 2 du bandeau de purepeople.fr le 1er juin 2020, permettant une configuration finalité par finalité, selon une liste établie dans le standard TCF, et disposant d'un bouton « tout refuser ».

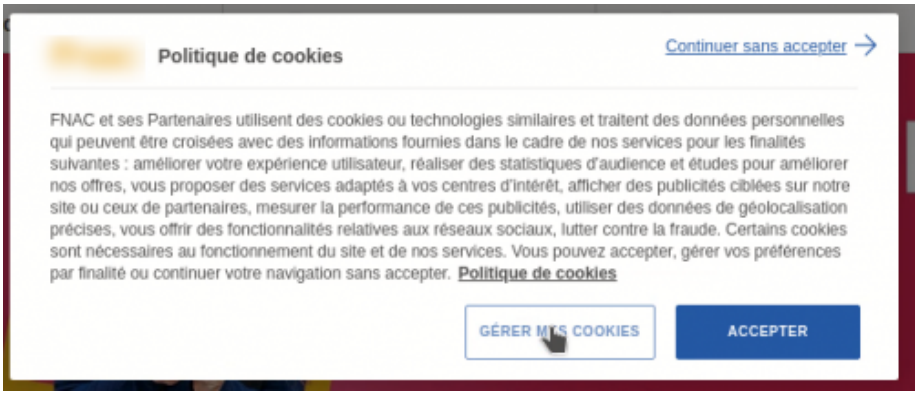
De nombreuses astuces ont été imaginées pour amener l'internaute à avoir une action interprétée (ou du moins interprétable) comme un consentement. C'est le cas par exemple des 31 % de sites en 2020 (contre 2 % en 2021) qui faisaient disparaître le bandeau comme si nous avions exprimé un consentement lorsque nous faisions simplement défiler la page avec le troisième bouton de la souris (fonction de scrolling).

Une autre évolution significative relève du fait que la proportions des bandeaux n'affichant pas dès l'étape 1 de signe passeur pour refuser tous les traceurs, accessible aussi facilement que celui destiné à exprimer un consentement, est passée de 99 % à 28 %.

Les dark patterns d'obstruction ont considérablement diminué, même s'ils n'ont pas tout à fait disparu. Là où 37 % des bandeaux étudiés en 2020 ne permettaient pas d'accéder à la lecture de la politique de confidentialité du site sans action de consentement, cette part n'était plus que de 4,5 % en 2021. Les duperies sont aussi en diminution. Les

bandeaux disparaissant dès que l'internaute poursuit sa navigation, même s'il n'a pas signifié de consentement au pistage, constituaient 58 % du total en 2020, contre 8 % en 2021.

Aujourd'hui, un bandeau cookie typique présente une forme et un texte qui mettent en scène le consentement comme étant un acte positif à défaut duquel il ne peut être supposé, comme dans l'exemple ci-dessous :



Capture d'écran de l'étape 1 du bandeau de la FNAC (logo flouté), daté du 1er juillet 2021.

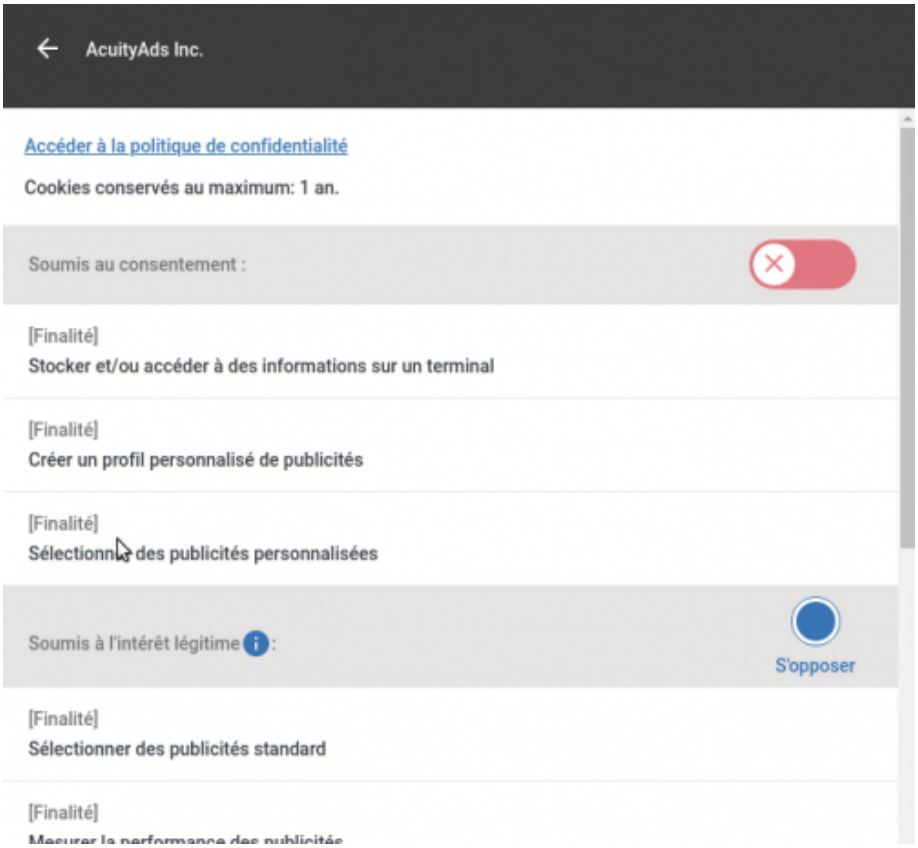
Dans le bandeau ci-dessus, nous voyons qu'il y a une mention des finalités pour lesquelles des cookies peuvent être déposés et des données personnelles traitées. Nous ne voyons pas de discours prétendant que « qui ne dit mot consent ». En revanche, le signe passeur permettant de refuser tous les pisteurs en une seule action dès l'étape 1 est un simple lien hypertexte portant l'étiquette « continuer sans accepter. » Il n'est pas au même niveau que le bouton permettant d'accepter. Les interférences n'ont donc pas totalement disparu.

… mais avec des nuances

En 2020, 67 % des bandeaux présentaient un design incitatif pour le bouton « j'accepte » en étape 1, contre 60,5 % environ en 2021. Cette proportion, étant donné la taille de notre corpus, doit donc être considérée comme stable. Il en va de même pour la proportion des sites qui cherchent à susciter la pitié de l'internaute, et de jouer sur les émotions, pour lui faire accepter le pistage de sa navigation ; elle est passée de 19 % en 2020 à 17 % en 2021, ce qui n'est pas une baisse significative. Les interférences d'interface sont, de façon générale, autant

présentes en 2021 qu'en 2020.

Une autre nuance à apporter au constat de très fort progrès de la conformité des bandeaux cookies entre 2020 et 2021 est l'apparition sur un nombre important de ceux-ci d'une distinction entre les traitements de données personnelles fondées sur le consentement, et ceux fondés sur l'intérêt légitime. En pratique, cela permet aux seconds de rester sur une logique d'*opt-out*. S'il est possible que certains traitements de données puissent effectivement se fonder sur l'intérêt légitime du responsable du traitement, nous avons vu précédemment que cela est très discutable pour ce qui concerne le pistage (même *stateless*[33]) à des fins publicitaires. Il est en outre imposé par l'article 13 (1) (d) du RGPD d'indiquer clairement aux personnes concernées par un traitement fondé sur l'intérêt légitime la nature de cet intérêt, d'une façon qui, selon l'article 12 du même règlement, doit être « concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. » Or, les options d'opt-out aux intérêt légitimes sont souvent cachées derrière plusieurs étapes d'interaction. Dans l'exemple ci-dessous, nous voyons ainsi cet intérêt légitime n'apparaître qu'après un ou plusieurs clics :

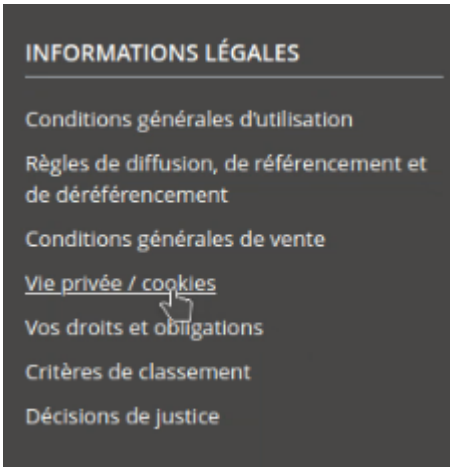


Capture d'écran du bandeau cookie de lefigaro.fr prise le 24 juin 2021, où

l'intérêt légitime n'apparaît qu'au bout de trois clics.

Semblant prendre appui sur la jurisprudence du Conseil d'État affirmant qu'il convient d'apprécier au cas par cas si le fait d'être empêché d'accéder à un site présente un « inconvénient majeur » susceptible d'interdire la pratique du *cookie wall*, une nouvelle forme d'action forcée qui s'est développée en 2021 consiste à proposer un paiement comme seule alternative à l'acceptation de l'ensemble des traceurs. C'est ce que pratique notamment le site allocine.fr. D'autres sites, comme lemonde.fr, affichent un bandeau couvrant une large part du contenu et appelant l'internaute à s'abonner s'il n'accepte pas tous les traceurs proposés par le bandeau cookie, ce qui constitue une interférence d'interface[34].

Enfin, non seulement tous les sites ne permettent pas de retirer un consentement donné, mais ceux qui permettent de revenir paramétrer ses choix en matière de pistage cachent généralement cette option via un lien caché dans le footer (le bas) de la page, comme dans l'exemple ci-dessous :



Capture d'écran du footer du site leboncoin.fr prise le 23 juin 2021.

Cela constitue aussi une forme d'interférence d'interface, dont nous n'avons toutefois pas évalué la prévalence, faute de critères objectivables permettant de définir la « facilité » du retrait du consentement.

Quelle influence de la CMP ?

Nous avions fait l'hypothèse, initialement, que les CMP jouaient un rôle déterminant dans le degré de conformité d'un bandeau, et dans le type de

consentement qu'il incarne. Si le standard TCF a considérablement standardisé les textes des options de paramétrage du consentement par finalité, généralement disponible en cliquant sur un bouton de type « paramétrer les cookies », l'IAB, qui édicte cette norme, s'est gardée d'imposer aux sites utilisant des CMP une interprétation des règles de droit applicables au consentement en matière de cookies et de traitement de données personnelles, pour se décharger de la responsabilité de ce choix (Santos et al., 2021).

Ainsi, en 2020, nous n'avions pas trouvé de corrélation significative entre la CMP choisie, et le nombre des critères de conformité retenus dans cette étude qui étaient enfreints :

Type de bandeau cookie	**Nombre moyen de critères de conformité enfreints**
Tous bandeaux confondus (n = 90)	3,24
Sites avec CMP, tous CMP confondus (n = 52, avec AdChoices)	3,48
Sites avec CMP conforme au TCF (n = 47)	3,53
Didomi (n = 14)	2,79
Commanders Act (n = 6)	4,17
Sourcepoint (n = 5)	3,80

Les textes présentés à l'internaute arrivant sur un bandeau cookie pour la première fois n'étaient pas non plus déterminés par la CMP. Ainsi, la similarité entre ces textes restait faible :

Proportion de texte identique par paire de bandeaux (1 = 100 % identique) en 2020			
Groupe	**Moyenne**	**écart-type**	**Nombre de paires**
Tous les bandeaux cookies	0.159	0.120	4005
COMMANDERS_ACT	0.330	0.187	15
DIDOMI	0.220	0.166	91
SOURCEPOINT	0.608	0.375	10

La seule exception à cela est le cas de Sourcepoint, mais quatre des cinq bandeaux générés par Sourcepoint dans notre corpus de 2020 provenaient de sites appartenant au même groupe de presse : Prisma Media. Ce ne serait donc pas tant le CMP qui imposerait un texte unique sur l'ensemble des bandeaux qu'il génère, mais le fait que deux sites appartiennent au même propriétaire qui tendrait à ce que les textes affichés sur leurs bandeaux se ressemblent, voire sont identiques.

Site 1	Site 2	Ratio (1.0 = 100 % identique)	Groupe
journaldesfemmes.fr	linternaute.com	1.0	Groupe Figaro CCM Benchmark
journaldesfemmes.fr	commentcamarche.net	1.0	Groupe Figaro CCM Benchmark
linternaute.com	commentcamarche.net	1.0	Groupe Figaro CCM Benchmark
office.com	microsoft.com	1.0	Microsoft
cuisineaz.com	rtl.fr	0.995372018512	Groupe M6
google.com	youtube.com	0.993049763692	Alphabet
gala.fr	capital.fr	0.989231522271	Prisma Media
leparisien.fr	lesechos.fr	0.986243386243	Groupe Les Échos-Le Parisien
programme-tv.net	gala.fr	0.983694329521	Prisma Media
gala.fr	femmeactuelle.fr	0.982498784638	Prisma Media
allocine.fr	purepeople.com	0.98049319102	Webedia
xvideos.com	xnxx.com	0.979702790866	WGCZ Holding
femmeactuelle.fr	capital.fr	0.979641299079	Prisma Media
ouest-france.fr	actu.fr	0.979304959	Groupe SIPA-Ouest-France
programme-tv.net	femmeactuelle.fr	0.974210653169	Prisma Media
programme-tv.net	capital.fr	0.964329046348	Prisma Media
public.fr	programme-television.org	0.960088691796	Prisma Media

Ces constats nous conduisent à questionner les dynamiques qui se tiennent entre les directions juridiques des entreprises (auxquelles appartiennent les sites étudiés) et les autres corps professionnels (développeurs des sites, développeurs de CMPs, rédactions…) en ce qui concerne la définition des contenus affichés sur un bandeau cookie. Il s'agirait de mieux saisir la chaîne éditoriale de ces bandeaux cookies.

Conclusions et pistes de recherche

La première phase du projet WebConsentement, financé par l'Université Rennes 2, le PREFICS et le LIRIS, nous permet d'aboutir à trois conclusions.

D'abord, aucun bandeau cookie étudié en 2020 n'était pleinement conçu pour recueillir un consentement défini par le RGPD comme étant notamment libre, éclairé, dépourvu d'ambiguïté, ou, en d'autres termes, en phase avec l'expression selon laquelle « si c'est pas oui, c'est non. » Ils incarnaient en revanche l'une de ces deux autres conceptions concurrentes du consentement : celle selon « qui ne dit mot consent » (consentement tacite), voire un consentement stoïcien, où il n'est possible que de s'informer sur son sort.

Ensuite, les *dark patterns* qui biaisent l'expression d'un consentement au sens du RGPD n'ont pas totalement disparu en 2021. Toutefois, le passage à la version 2.0 du TCF, mais surtout des décisions de justice et d'autorités de contrôle, semblent avoir eu pour effet d'entraîner une conformité bien plus forte en 2021 qu'en 2020 aux règles sur le

consentement qui résultent de la lecture conjointe de la directive e-Privacy de 2002 et du RGPD.

Enfin, les CMPs utilisés par les bandeaux de notre corpus semblent offrir une large liberté éditoriale aux personnes qui les configurent, cependant, au moins dans le domaine de la presse en ligne, nous observons de grandes similarités de configuration. Ainsi, cette dernière, semble s'opérer sous le joug d'une logique de centralisation, fruit d'une logique d'économie d'échelle et d'une rationalisation organisationnelle et non de manière distribuée dans les différentes rédactions. Les choix de configuration présentés en seconde étape d'interaction des bandeaux conformes au TCF doivent toutefois respecter les règles de ce standard en matière d'énonciation des différentes finalités pour lesquelles des pisteurs peuvent être activés et des données personnelles traitées.

Une simple étude sur corpus ne permet pas de comprendre de façon exhaustive la chaîne éditoriale qui va de la Loi, au standard (comme le TCF), au logiciel qui génère le bandeau et doit garantir le respect du choix exprimé par l'internaute (le CMP, lorsqu'il y en a un), à l'apparence visuelle du bandeau, aux choix de paramétrage de sa forme et des interactions, aux textes qui sont affichés sur le bandeau et dans la politique de confidentialité associée. Qui sont les acteurs de cette chaîne ? Où, et en fonction de quels critères, se prennent les décisions ? Quels sont les mécanismes de réception du droit qui expliquent celles-ci ? Les choix se font-ils en rapport avec des convictions personnelles sur le consentement ?

Une prochaine étape du projet WebConsentement consistera donc à interroger des acteurs de cette chaîne éditoriale, depuis une perspective communicationnelle du droit, et en nous interrogeant sur l'existence ou non d'un paradoxe de la vie privée au niveau des développeurs, designers et autres professionnels impliqués.

Ce paradoxe, pensé en référence au « paradoxe de la vie privée » mis en évidence et discuté par de nombreux travaux (Acquisti et Gross, 2006 ; Estienne, 2011 ; Gerber, Gerber et Volkamer, 2018 ; Hémont et Gout, 2020 ; Norberg, Home et Home, 2007), voudrait que les développeurs (et les autres professionnels du web), bien qu'attachés/sensibilisés au droit à la vie privée comme droit individuel et collectif, développent des services qui, par conception, mettent en péril la vie privée de leurs utilisateurs. Les études à ce sujet sont encore rares (voir par exemple :

Tahaei et Vaniea, 2021 ; Tahaei, Vaniea et Saphra, 2020), et ne concernent pas encore, à notre connaissance, les bandeaux cookies, ni la question du consentement comme norme morale de régulation des rapports sociaux.

Nous menons également une étude auprès d'un panel d'internautes pour étudier la réception des bandeaux cookies, selon une perspective inspirée des travaux de Stuart Hall sur le codage et le décodage des messages médiatiques (Hall, 1994). Ces entretiens, dont une première partie est actuellement en cours de retranscription, semble suggérer que l'avènement de boutons qui (quoique souvent peu mis en valeur) permettent de refuser les « cookies » et autres traceurs aussi facilement, accorde à de nombreuses personnes la possibilité de se saisir de cette nouvelle capacité d'action afin d'agir en réaction au sentiment d'intrusion ressenti de longue date face au pistage de leur navigation et à la captation de leurs données à caractère personnel. Il semblerait que, chez la majorité de nos enquêtés, le refus du pistage soit devenu un automatisme découlant du manque de confiance envers l'industrie du Web. Si cette hypothèse se confirmait, cela validerait la stratégie du législateur européen consistant à faire du consentement individuel un instrument de résistance et négociation collectives aux modèles d'affaires qui s'épanouissent de la prédation sur des données à caractère personnel pouvant révéler des informations particulièrement sensibles sur la vie des internautes.

Ces prochaines étapes du projet WebConsentement donneront lieu à de futures communications.

Bibliographie

Acquisti A., Gross R., 2006, « Imagined Communities : Awareness, Information Sharing, and Privacy on the Facebook », *Proceedings of the 6th International Conference on Privacy Enhancing Technologies*, p. 36-58.

Brignull H., non daté. « Tricks used in websites and apps that make you buy or sign up for things that you didn't mean to », Dark Patterns. En ligne : [https://darkpatterns.org/] (page consultée le 6 octobre 2020).

Chaves Ferreira B., Jourdain A., Naulin S., 2018, « Les plateformes numériques révolutionnent-elles le travail ?Une approche par le web scraping des plateformes Etsy et La Belle Assiette », *Réseaux*, 212, 6, p. 85-119.

Christelle M., 2014, *Consentement et subjectivité juridique : contribution à une théorie émotivo-rationnelle du droit*, Thèse de doctorat, Paris, Université Paris 1.

Comité européen de protection des données, 25 mai 2018, Déclaration du comité européen de la protection des données sur la révision de la directive ePrivacy et son incidence sur la protection de la vie privée et la confidentialité des communications électroniques.

Comité européen de protection des données, 2020 (19 novembre). « Subject : Letter of 13 July 2020 from News Media Europe and others », référence OUT2020-0122.

Commission européenne. 2012 (25 janvier), Proposition de Règlement relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, document COM (2012) 11 FINAL.

Cousin C., 2016, *Vers une redéfinition de l'acte médical*, Thèse de doctorat, Rennes, Université Rennes 1.

Degeling M., Utz C., Lentzsch C., Hosseini H., Schaub F., Holz T., 2019, « We Value Your Privacy ... Now Take Some Cookies : Measuring the GDPR's Impact on Web Privacy », *Proceedings 2019 Network and Distributed System Security Symposium*.

EDPB (Comité européen de protection des données – European Data Protection Board), 2023, *Draft Report of the work undertaken by the Cookie Banner Taskforce*, https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf

Englehardt S., Narayanan A., 2016, « Online Tracking:A 1-million-site Measurement and Analysis », CCS '16 : Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, https://dl.acm.org/doi/10.1145/2976749.2978313.

Estienne Y., 2011, « Un monde de verre : Facebook ou les paradoxes de la vie privée (sur)exposée », *Terminal*. Technologie de l'information, culture & société, 108-109, p. 65-84.

Fraisse G., 2017, *Du consentement : essai : suivi d'un épilogue inédit Et le refus de consentir ?*, édition augmentée, Paris, Éditions du Seuil.

Frison-Roche M.-A., 1995, « Remarques sur la distinction de la volonté et du consentement en droit des contrats », *Revue trimestrielle de droit civil*, 3, p. 573-578.

Gerber N., Gerber P., Volkamer M., 2018, « Explaining the privacy paradox : A systematic review of literature investigating privacy attitude and behavior », *Computers & Security*, 77, p. 226-261.

Gray C.M., Kou Y., Battles B., Hoggatt J., Toombs A.L., 2018, « The Dark (Patterns) Side of UX Design », Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18, p. 1-14.

Gray C., Santos C., Bielova N., Toth M., Clifford D., 2021, « Dark Patterns and the Legal Requirements of Consent Banners : An Interaction Criticism Perspective », ACM CHI Conference on Human Factors in Computing Systems.

Groupe de travail de l'Article 29 (G29), 2 octobre 2013, « Working Document 02/2013 providing guidance on obtaining consent for cookies », https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

Groupe de travail de l'Article 29 (G20), 2014, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE.

Hall S., 1994, « Codage/décodage », *Réseaux*, 12, 68, p. 27-39.

Hémont F., Gout M., 2020, « Consentement résigné : en finir avec le Privacy Paradox », dans Turgis S., Boizard M., Bensamoun A. (dirs.), *Le profilage en ligne : entre libéralisme et régulation*, Editions Mare et Martin.

Jeanneret Y., Souchier E., 2005, « L'énonciation éditoriale dans les écrits d'écran », *Communication & Langages*, 145, 1, p. 3-15.

Kristol D.M., 2001, « HTTP Cookies : Standards, privacy, and politics », ACM Transactions on Internet Technology, 1, 2, p. 151-198.

Laugier S., 2004, « Performativité, normativité et droit », *Archives de Philosophie*, Tome 67, 4, p. 607-627.

Matte C., Bielova N., Santos C., 2020, « Do Cookie Banners Respect my Choice ? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework », SP 2020 - IEEE Symposium on Security and Privacy, p. 791-809.

Norberg P.A., Home D.R., Home D.A., 2007, « The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors », *Journal of Consumer Affairs*, 41, p. 100-126.

Nouwens M., Liccardi I., Veale M., Karger D., Kagal L., 2020, « Dark Patterns after the GDPR : Scraping Consent Pop-ups and Demonstrating their Influence », Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, p. 1-13.

Olejnik L., Castelluccia C., 2014, « To bid or not to bid ? Measuring the value of privacy in RTB », https://lukaszolejnik.com/rtb2.pdf.

Rossi J., 2021, « What rules the Internet ? A study of the troubled relation between Web standards and legal instruments in the field of privacy », *Telecommunications Policy*, 45, 6, p. 102143.

Santos C., Bielova N., Matte C., 2019, « Are cookie banners indeed compliant with the law ? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners », papier publié sur arXiv.org https://arxiv.org/pdf/1912.07144.pdf (publié en 2020 dans *Technology and Regulation*, p. 91–135).

Santos C., Nouwens M., Toth M., Bielova N., Roca V., 2021, « Consent Management Platforms under the GDPR : processors and/or controllers ? », *Privacy Technologies and Policy*, 9th Annual Privacy Forum, p. 47-69.

Sarthou-Lajus N., 2009, « Du goût pour les stoïciens », *Etudes*, 410, 6, p. 775-786.

Souchier E., 1996, « L'écrit d'écran, pratiques d'écriture & informatique », *Communication et langages*, 107, 1, p. 105-119.

Tahaei M., Vaniea K., 2021, « "Developers Are Responsible" : What Ad Networks Tell Developers About Privacy », CHI EA '21 : Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, p. 1-11.

Tahaei M., Vaniea K., Saphra N., 2020, « Understanding Privacy-Related Questions on Stack Overflow », Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, p. 1-14.

Toubiana V., Narayanan A., Boneh D., Nissenbaum H., Barocas S., 2010, « Adnostic : Privacy Preserving Targeted Advertising », Proceedings Network and Distributed System Symposium.

Utz C., Degeling M., Fahl S., Schaub F., Holz T., 2019, « (Un)informed Consent : Studying GDPR Consent Notices in the Field », 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 2019.

Verbeek P.-P., 2006, « Materializing Morality : Design Ethics and Technological Mediation », *Science, Technology, & Human Values*, 31, 3, p. 361-380.

Waldman A.E., 2020, « Cognitive biases, dark patterns, and the 'privacy paradox' », *Current Opinion in Psychology*, 31, p. 105-109.

Zuiderveen Borgesius F., 2015, « Personal Data Processing for Behavioural Targeting : Which Legal Basis ? », *International Data Privacy Law*, 5, 3, p. 163–176.

Zuiderveen Borgesius F., 2016, « Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation », *Computer Law & Security Review*, 32, 2, p. 256-271.

---

1 Pour une histoire des cookies, voir : Kristol 2001.

2 Traduit de l'anglais. Texte original : « A cookie banner is a mean for getting user's consent on the usage of cookies and potentially other web application technologies that can store data or use browser attributes to recognize the user's browser, such as browser fingerprinting. »

3 Au sens des théories des actes de langage. Voir : Laugier, 2004.

4 Voir la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

5 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

6 Règlement 2016/679/UE du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

7 CE 10e et 9e ch., 19 juin 2020, Association des agences-conseils en communication et autres, n° 434684.

8 CJUE 1er octobre 2019, Planet49, aff. C-673/17 et CJUE 11 novembre 2020, Orange Roumanie, aff. C-61/19.

9 La technique du web scraping est décrite ici dans Chaves Ferreira, Jourdain et Naulin, 2018.

10 Ce terme désigne les noms de domaine qu'il est possible d'achter, comme exemple.fr, et au contraire de exemple.exemple.fr.

11 CJUE 1er octobre 2019, Planet49, aff. C-673/17, pt. 57.

12 CJUE 11 novembre 2020, Orange Roumanie, aff. C-61/19.

13 Voir la fiche disponible sur le site de la CNIL, en date du 24 février 2020 : https://www.cnil.fr/fr/dispositifs-de-mesure-daudience-et-de-frequentation-dans-des-espaces-accessibles-au-public-la-cnil .

14 CJUE 1er octobre 2019, Planet49, aff. C-673/17.

15 Conseil d'État, 9e et 10e sections réunies, Association des agents-conseils en communication et autres, n° 434684, pt. 15.

16 Voir : CJUE 10 décembre 2018, Wightman e.a., C-621/18, pt. 47 ; CJUE 27 novembre 2012, Thomas Pringle, C-370/12, pt. 135 ; CJCE 17 novembre 1983, Firma E. Merck contre Hauptzollamt Hamburg-Jonas, aff. 292/82.

17 Traduit de l'anglais : « generally, the user should retain the possibility to continue browsing the website without receiving cookies ».

18 Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs).

19 Conseil d'État, 9e et 10e sections réunies, Association des agents-conseils en communication et autres, n° 434684, pt. 10.

20 En particulier les amendements 202, 498 et 499. Voir la liste des amendements sur : https://www.europarl.europa.eu/doceo/document/A-9-2021-0356_EN.html (page consultée le 25 janvier 2022).

21 Voir : article 8 de la proposition de Règlement européen concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE de la Commission européenne : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52017PC0010&from=EN (page consultée le 25 janvier 2022).

22 Voir le considérant 20 du projet de règlement e-Privacy.

23 Voir : amendement 23 du projet de rapport sur la proposition de Règlement européen concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques du 9 juin 2017, rédigé par Marju Lauristin. https://www.europarl.europa.eu/doceo/document/LIBE-PR-606011_EN.pdf (page consultée le 25 janvier 2022).

24 Voir : https://globalprivacycontrol.org/ (page consultée le 25 janvier 2022).

25 Voir : https://www.dataprotectioncontrol.org/adpc-spec/ (page consultée le 25 janvier 2022).

26 Voir le document 6087/21 du 10 février 2021 du Conseil de l'UE : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN (page consultée le 25 janvier 2021).

27 Code disponible sur GitHub : https://github.com/Perdu/Cookie-Glasses (page consultée le 26 janvier 2021).

28 L'extension d'origine peut être téléchargée ici : https://chrome.google.com/webstore/detail/cookie-glasses/gncnjghkclkhpkfhghcbobednpchjifk (page consultée le 22 septembre 2022)

29 Voir les spécifications disponibles sur Github : https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20CMP%20API%20v2.md (page consultée le 22 septembre 2022)

30 Les iframes sont des éléments dans le code d'une page web qui permettent d'imbriquer une autre page web dans celle-ci.

31 La liste est disponible à l'adresse : https://iabeurope.eu/cmp-list/ (page consultée le 26 janvier 2021).

32 Décision 21/2022 du 2 février 2022 de la Chambre contentieuse de l'Autorité de protection des données de Belgique.

33 C'est-à-dire sans enregistrement sur le terminal de l'utilisateur

34 Postérieurement à la fin de la rédaction de ce papier, lemonde.fr a adopté le modèle du « cookie pay wall » que des sites comme Allocine.fr avaient déjà adopté.

+

Le code source du plug-in que nous avons utilisé est en ligne sur https://www.julienrossi.com/documents/cookies_plugin . Ce plug-in est bricolé, et ne peut pas être considéré comme une version pleinement aboutie. Il est une adaptation à la version 2 du standard TCF du plug-in Cookie Glasses, rédigé par Célestin Matte, est disponible ici : https://github.com/Perdu/Cookie-Glasses .