



HAL
open science

Cookies et autres traceurs : des sanctions pour les géants du numérique, mais des leçons pour tous

Emmanuel Netter

► **To cite this version:**

Emmanuel Netter. Cookies et autres traceurs : des sanctions pour les géants du numérique, mais des leçons pour tous. RTDCom. Revue trimestrielle de droit commercial et de droit économique, 2022, 02, pp.295. halshs-03735564

HAL Id: halshs-03735564

<https://shs.hal.science/halshs-03735564>

Submitted on 9 Feb 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Cookies et autres traceurs : des sanctions pour les géants du numérique, mais des leçons pour tous

RTD. Com. 2022/2

Emmanuel Netter
professeur de droit privé à l'université d'Avignon

CNIL, délibération SAN-2021-023 du 31 décembre 2021

CNIL, délibération SAN-2021-024 du 31 décembre 2021

Conseil d'État, 10ème - 9ème chambres réunies, 28 janvier 2022, 449209

Nombreuses sont les entreprises qui offrent des services à leur clientèle, ou plus simplement communiquent avec elles par l'intermédiaire d'un site internet ou d'une application pour smartphone. Ces interfaces constituent des outils numériques de la vie des affaires, ce qui justifie leur inclusion dans cette nouvelle chronique. Or, il est fréquent que ces sites internet ou applications mobiles procèdent à des opérations de lecture et d'écriture d'informations dans les terminaux des utilisateurs. La question est connue comme celle des « cookies » même si, techniquement, les cookies ne constituent qu'une des variétés de traceurs susceptibles d'être utilisés en pareil contexte. Il faut alors prendre garde à une directive européenne de 2002 sur le traitement de données personnelles dans le secteur des communications électroniques, dite aussi « e-privacy »¹, telle qu'elle a été transposée en droit interne à l'article 82 de la loi informatique et libertés (LIL)². En substance, ce texte exige, avant tout accès ou inscription dans la mémoire du terminal, que l'on informe correctement l'internaute sur les finalités des traceurs, et que l'on recueille son consentement. Les exceptions sont étroites : elles ne bénéficient qu'au cookie ayant « pour finalité exclusive de permettre ou faciliter la communication par voie électronique » ou « strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur ». Tous les traceurs à finalité publicitaire sont à l'évidence concernés par cette double exigence d'information et d'autorisation. Or, les grandes entreprises américaines ne sont pas les seules à « monétiser » leur audience et à pratiquer, par elles-mêmes ou en partenariat, des formes diverses de publicité personnalisée. La presse en ligne, nationale aussi bien que régionale, en constitue un exemple. Même certains cookies dits « de mesure d'audience » sont susceptibles d'être soumis à acceptation, si leur sophistication les fait sortir du champ étroit des exceptions légales³. Cette question des traceurs doit donc faire l'objet d'une attention particulière des directions juridiques, et constituer à elle seule un chapitre de la démarche de mise en conformité avec la réglementation en matière de données à caractère personnel.

À cet égard, trois décisions récentes méritent d'être présentées ensemble aux lecteurs. Celle qui a été rendue par le Conseil d'État le 28 janvier dernier examinait un recours formé par Google contre une sanction de 100 millions d'euros qui lui avait été infligée par la CNIL en décembre 2020 en raison de sa politique en matière de cookies – une amende de 35 millions d'euros avait été prononcée contre Amazon pour des motifs quasiment identiques⁴. Il s'agissait alors, d'une part de contrôler si l'internaute était correctement informé des raisons d'être des traceurs que l'on s'apprêtait à déposer sur son appareil, d'autre part de s'assurer que l'utilisateur disposait d'un pouvoir effectif de refuser.

1 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

2 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

3 V. l'art. 5 des lignes directrices de la CNIL sur les cookies (délibération n° 2020-091).

4 CE, 28 janvier 2022, n° 449209 : Dalloz actualité, 22 avril 2022, obs. C. Crichton ; Dalloz IP/IT, note à paraître T. Douville, rendu sur recours contre CNIL, Délib. SAN-2020-012 du 7 décembre 2020 : CCE, avril 2021, obs. A. Danis-Fatôme ; Dalloz IP/IT, nos obs.

Quant aux deux délibérations de la CNIL du 31 décembre 2021, elles posent une question différente⁵. Dans ces deux cas, il était acquis que l'utilisateur pouvait refuser les cookies, dont les finalités lui avaient été correctement présentées. Restait à savoir *comment* il lui fallait matérialiser ce refus. En effet, le « bandeau cookies » - nom donné par la pratique à l'interface qui permet à l'internaute d'indiquer ses choix – des sociétés concernées rendait le refus un peu plus long et plus complexe que l'acceptation des traceurs. Aussi des amendes ont-elles été infligées à Facebook, à hauteur de 60 millions d'euros, et à deux sociétés du groupe Google /Alphabet à nouveau, pour un montant record de 150 millions d'euros.

Avant d'aborder la question des traceurs à proprement parler (II), les trois décisions accordent une place importante au mécanisme de « guichet unique », fort décrié, que le RGPD prévoit en cas de traitements impliquant plusieurs pays de l'Union européenne. C'est l'occasion de revenir sur cette question, qui menace à elle seule de paralyser l'efficacité du droit européen des données personnelles (I).

I – L'inapplicabilité du « guichet unique » à la question des cookies

Lorsqu'un traitement de données à caractère personnel est « transfrontalier », c'est-à-dire qu'il concerne plusieurs pays de l'Union, il pourrait sembler regrettable de laisser les autorités de protection agir en ordre dispersé. Afin d'assurer un traitement homogène et cohérent du dossier, mais aussi dans l'intérêt du responsable de traitement mis en cause – qui bénéficiera ainsi d'un interlocuteur unique – il est donc instauré par le RGPD un mécanisme « d'autorité chef de file », dit aussi « guichet unique » ou « one-stop-shop »⁶.

Séduisante en théorie, l'idée a tout simplement tourné au désastre. La plupart des très grandes sociétés américaines du numérique ont localisé à Dublin leur centre de décision européen en matière de données personnelles (notamment Google, Microsoft, Apple et Facebook – Amazon dépendant quant à lui du Luxembourg). Or, le *Data Protection Commissioner* (DPC) a fait la démonstration constante de sa mauvaise volonté dans l'instruction des plaintes déposées auprès de ses services. Ses moyens sont certes largement sous-dimensionnés : une petite équipe travaillant dans un local minuscule à côté d'une supérette⁷. Mais au moins aurait-elle pu dédier ses maigres ressources à un traitement correct des principaux dossiers. Ce n'est pas le cas : les plaintes déposées par Max Schrems, la star autrichienne de la défense des données personnelles, contre Facebook, datent de ses années à présent lointaines d'étudiant en droit et n'ont toujours pas connu leur dénouement⁸. Sans que le lien de cause à effet puisse être démontré, la contribution très significative des « GAFAM » au PIB irlandais est parfois soupçonnée d'être à l'origine des comportements velléitaires de l'autorité irlandaise. Toujours est-il qu'un « Big Brother Award » vient d'être attribué au DPC par un jury comprenant notamment la Ligue des Droits de l'Homme et l'Association allemande pour la protection des données⁹.

Pour les entreprises basées dans d'autres pays européens, dont la France, une telle situation va jusqu'à poser des questions en matière de loyauté de la concurrence : les acteurs dépendant de l'Irlande peuvent, de fait, se dispenser de respecter le droit des données personnelles et par conséquent s'épargner le coût – non négligeable à bien des égards – de la mise en conformité. C'est

5 CNIL, délibérations SAN-2021-023 et SAN-2021-024 du 31 décembre 2021 : Dalloz IP/IT, 2022, p. 7, note C. Crichton ; CCE, 2022, comm. n° 22, obs. L. Maisnier-Boché.

6 Sur lequel V. F. Jault-Seseke, « Protection des données : la mise en œuvre du guichet unique ou les limites de l'intégration européenne », RTD. Eur., 2022, p. 81.

7 V. les images et la description de J.-M. Manach, « La CNIL irlandaise écope d'un Big Brother Awards », article nextinpact.com du 2 mai 2022.

8 Les plaintes datent de 2013. V. par ex. « Irish High Court allows Judicial Review aiming to stop Facebook's EU-US Data Transfers » sur noyb.eu.

9 J.-M. Manach, art. préc.

aussi et surtout le respect des droits fondamentaux des citoyens de l'Union, y compris français, qui est menacé par l'inaction de l'autorité irlandaise.

On comprend donc que la CNIL française soit à l'affût de la moindre occasion de contourner le si défaillant « guichet unique », en attendant qu'il soit peut-être réformé un jour par le législateur européen. Elle était parvenue à le faire très ponctuellement en janvier 2019, en infligeant à Google une amende de 50 millions d'euros¹⁰. En résumé, l'entreprise américaine avait alors situé ses intérêts européens en Irlande de manière insuffisamment nette. La CNIL avait vu la faille et l'avait exploitée. La brèche a été refermée depuis et, lorsqu'il s'agit d'appliquer le RGPD à Google, l'Irlande a malheureusement repris la main.

Mais il en va différemment lorsqu'il est question de mettre en oeuvre la directive sur les communications électroniques, texte spécial par rapport à la législation générale et transectorielle qu'est le RGPD. Elle ne contient aucune référence au guichet unique. Il n'en fallait pas davantage à la CNIL pour considérer qu'en matière de cookies et autres traceurs, chaque autorité nationale est libre de ses poursuites : c'est en ce sens qu'elle s'est prononcée dès les sanctions précitées de 2020 contre Google et Facebook. Fin 2021, la CNIL infligeait de nouvelles amendes, touchant une nouvelle fois aux cookies, mais pour des manquements, on l'a dit, d'une autre nature. Le Conseil d'État n'avait pas encore statué sur le recours formé contre les sanctions de 2020, c'est pourquoi l'autorité française et les géants américains ont engagé un nouveau bras de fer sur la question.

L'argumentation déployée par Google, Facebook - et par Amazon un an plus tôt - peut se résumer comme suit : en 2002, le guichet unique n'avait pas encore été imaginé. On ne peut donc pas considérer que le texte sectoriel a refusé cette logique, qui n'existait pas alors, mais simplement qu'il est resté silencieux à son propos. Ce n'est qu'en 2016, avec l'adoption du RGPD (entré en application en 2018) qu'est apparue la figure du one-stop-shop. Elle aurait alors comblé un vide et aurait par conséquent été applicable même en matière de communications électroniques.

À ce raisonnement, la CNIL a opposé en 2020 et 2021 plusieurs réponses, dont la plus convaincante est celle-ci : le guichet unique fait appel, pour son fonctionnement, à un organe appelé le Comité Européen pour la Protection des Données (CEPD), qui réunit l'ensemble des 27 CNILs européennes. Sans le CEPD, le one-stop-shop est, de fait, impossible à mettre en oeuvre tel qu'il a été conçu par le RGPD. Or, dans le domaine précis des communications électroniques, chaque État membre a été laissé libre de confier l'application de la directive à son autorité de protection des données ou bien à son autorité compétente en matière de télécommunications (son ARCEP). Plusieurs pays ont opté pour la seconde branche de l'alternative. Ainsi est-il impossible, en matière de cookies, de réunir l'ensemble des CNILs, donc le CEPD. Un autre argument est avancé, qui pèse moins lourd, mais reste considérable : le règlement e-privacy, qui va bientôt succéder à la directive, est en cours de négociation, et suscite de vives discussions sur le point de savoir s'il faut y inclure un guichet unique. N'est-ce pas la preuve qu'il n'en existe pas en droit positif ?

Un mois à peine après les nouvelles sanctions, le Conseil d'État se prononçait sur le recours formé contre celles de 2020, et par là mettait un terme à la discussion. Refusant de poser à la CJUE une question préjudicielle tant le droit européen lui paraissait sans ambiguïté sur ce point, il rejoint la CNIL et affirme que, dans le domaine « e-privacy », le guichet unique n'existe pas¹¹.

10 délibération SAN-2019-001 du 21 janvier 2019 : CCE, 2019, n 5, p. 31 (1ère partie) et n° 6, p. 28, note N. Metallinos ; JCP G, 2019, n° 13, p. 608, obs. A. Bellotti ; Dalloz IP:IT, 2019, n° 3, p. 165, nos observations.

11 Considérant 12 de l'arrêt précité du 28 janvier 2022 : « si les conditions de recueil du consentement de l'utilisateur prévues par le règlement du 27 avril 2016 sont applicables aux opérations de lecture et d'écriture dans le terminal d'un utilisateur, il n'a pas été prévu l'application du mécanisme dit du " guichet unique " applicable aux traitements transfrontaliers, défini à l'article 56 de ce règlement, pour les mesures de mise en oeuvre et de contrôle de la directive 2002/58/CE du 12 juillet 2002, qui relèvent de la compétence des autorités nationales de contrôle en vertu de l'article 15 bis de cette directive ».

Aussi les lecteurs doivent-ils retenir qu'en matière de cookies, des poursuites sont susceptibles d'être engagées séparément par chaque autorité européenne de protection des données dès lors qu'il est procédé à des lectures et écritures d'information au sein des terminaux des utilisateurs nationaux. Il n'en devient que plus crucial encore de soigner la conformité des traitements en la matière, ce qui nous amène à laisser derrière nous la procédure pour aborder le fond.

II – L'information et le recueil du consentement des utilisateurs en matière de cookies

Les deux lots de sanctions prononcées par la CNIL l'ont amenée à se prononcer sur des aspects différents de l'article 82 de la LIL.

Les amendes de 2020, que nous considérons ici sous l'angle de leur confirmation en tous points par le Conseil d'État le 28 janvier dernier, portaient à la fois sur l'information qui doit être préalablement délivrée aux internautes et sur la prise en compte de leur consentement dans son principe même (A). Les sanctions de 2021, sur lesquelles nous reviendrons ensuite, portent sur la forme concrète employée pour recueillir le consentement des utilisateurs (B).

A – L'information préalable et l'aptitude même à refuser les traceurs

L'article 82 de la LIL pose que tout utilisateur d'un service de communications électroniques « doit être informé de manière claire et complète » à la fois de la finalité des opérations de lecture et d'écriture effectuées dans son terminal et « des moyens dont il dispose pour s'y opposer ». La formule initialement choisie par Google consistait en un simple bandeau d'information au pied de la page google.fr, intitulé « rappel concernant les règles de confidentialité », assorti d'un bouton « me le rappeler plus tard » et d'un autre « consulter maintenant ». L'utilisateur devait déduire de cette présentation lénifiante et discrète qu'une information importante était à portée de clic. Aurait-il eu la vigilance de cliquer sur « consulter maintenant », il n'aurait toujours pas été correctement informé, selon le Conseil d'État, des règles de confidentialité applicables aux cookies, ni de la possibilité de refuser qu'ils soient implantés sur son terminal. Pour en arriver à être véritablement averti, « il fallait faire défiler le contenu de toute la fenêtre, ne pas cliquer sur l'un des cinq liens hypertextes thématiques figurant dans le contenu, et cliquer sur le bouton " autres options " ».

Il n'était pas douteux qu'un tel procédé serait jugé totalement insuffisant. Cependant, une fois la procédure de sanction engagée, les services de Google avaient opté pour une interpellation plus vive de leurs utilisateurs, sous la forme d'une « fenêtre surgissante » (la francisation du terme anglais « pop-up »). Celle-ci, intitulée « avant de continuer », contenait des considérations générales sur l'usage de cookies. Pour véritablement savoir de quoi il retournait, il fallait délaisser le bouton « j'accepte » pour choisir celui qui était libellé « en savoir plus ». La CNIL et le Conseil d'État ont considéré que cela restait insuffisant. Depuis, la société a fini par se hisser au niveau d'exigence attendu, et le lecteur pourra faire l'expérience d'une visite de google.com. Il découvrira une fenêtre surgissante décrivant immédiatement, sans action supplémentaire de l'internaute, les différentes finalités des traceurs employés. Début mai 2022, celles-ci sont au nombre de six : assurer le fonctionnement des services, mesurer l'audience, améliorer la qualité des services, diffuser des annonces, proposer des contenus personnalisés, proposer des publicités.

Une fois la question de l'information préalable résolue, encore faut-il que l'internaute dispose d'une capacité effective à s'opposer au dépôt des traceurs. En 2020, un contrôle en ligne réalisé par les services de la CNIL avait révélé, tant pour Amazon que pour Google, que certains cookies publicitaires étaient déposés sur le terminal au moment où le bandeau destiné à choisir s'affichait. Il

n'était donc pas tenu compte de la réponse¹². Quiconque dispose des connaissances techniques nécessaires constate que de telles pratiques sont assez répandues en ligne. Un manquement aussi grossier ne laisse guère d'espace aux responsables de traitement pour se défendre.

Google avait bien tenté de faire valoir « que le cadre juridique applicable aux cookies n'aurait pas été consolidé à la date de la décision attaquée ». Mais l'argument était faible. S'il est vrai que les lignes directrices de la CNIL étaient relativement récentes, les violations ici discutées touchent clairement et directement au cadre juridique préexistant.

Laissons là les sanctions de 2020, dont le souvenir est ravivé par la décision du Conseil d'État et considérons à présent celles qui ont été prononcées à la fin de l'année 2021. Cette fois-ci, il n'était pas reproché à Google et à Facebook de priver leurs utilisateurs d'une possibilité effective de refuser les traceurs. C'est la forme concrète selon laquelle ils sont interrogés et doivent répondre qui est à l'étude, autrement dit la manière dont se présente le « bandeau cookies ».

B – Les modalités concrètes de refus des traceurs

Les exigences de la CNIL en la matière sont connues. Ses fameuses lignes directrices exigent qu'il soit aussi simple de refuser les cookies que de les accepter¹³. La plupart des acteurs de taille plus modeste se sont pliés à l'exigence, en accompagnant les deux boutons classiques « tout accepter » et « personnaliser » d'une mention « continuer sans accepter ». Cette dernière est parfois rendue la plus discrète possible, en jouant sur le type de police, sa taille, sa couleur et sa localisation. De telles pratiques laissent d'ailleurs craindre que les prochaines décisions de la CNIL en matière de cookies ne sombrent dans d'affreuses discussions sur les détails, qui rappelleraient aux spécialistes de droit des affaires les pires arrêts en matière de mentions manuscrites dans les cautionnements délivrés par des personnes physiques à des créanciers professionnels.

En l'espèce, l'approche est largement simplifiée par le fait que Facebook et Google ne proposent aucun bouton de refus des traceurs « de premier niveau », c'est-à-dire immédiatement disponible sur le bandeau, sans qu'il soit nécessaire d'ouvrir préalablement une nouvelle fenêtre. Non seulement Google relègue la possibilité de refus au second niveau, mais il faut encore activer trois boutons à bascule puis confirmer l'opération. Les sociétés ne pouvaient pas douter, ce faisant, qu'elles contrevenaient frontalement aux attentes de la CNIL. Aussi plaident-elles plutôt que ni la directive sectorielle e-privacy, ni le droit commun des données personnelles que constitue le RGPD n'exigent ce bouton de refus au premier niveau des bandeaux cookies.

C'est exact, mais il ne revenait pas à ces textes de s'abaisser à des précisions aussi triviales. En définissant le consentement comme une « manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair (...) », le RGPD s'oppose à toute forme de biais. Or, on ne peut s'empêcher de penser que si les responsables de traitement rechignent tant à proposer au premier niveau deux boutons de même taille et de même couleur, l'un permettant d'accepter, l'autre de refuser, c'est pour de bonnes raisons. S'ils rusent, s'ils louvoient, s'ils demandent à leurs spécialistes des interfaces utilisateurs d'utiliser toute une gamme des « dark patterns », si certains d'entre eux plaident avec tant d'acharnement devant la CNIL puis le Conseil d'État, c'est bien que ces simples boutons ont un véritable impact. Dans ses décisions, la Commission s'était d'ailleurs appuyée sur des études universitaires démontrant – sans surprise – l'importante différence de taux de refus que l'on observe dès lors qu'on implémente un bandeau « loyal ». Ajoutons que Laboratoire d'Innovation de la CNIL avait étudié la

12 Dans le cas de Google, on relevait même qu'un cookie publicitaire continuait à fonctionner après une opposition explicite de l'utilisateur.

13 Délibération précitée n° 2020-091 : « (...) la Commission rappelle que, conformément à l'article 7.3 du RGPD, il doit être aussi simple de retirer son consentement que de le donner ».

question dans son guide « la forme des choix » (Cahier IP 6 du 20 mars 2019). Le Comité européen pour la protection des données a quant à lui publié récemment un projet de lignes directrices intitulé « Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them ».

L'approche de la CNIL consistant à exiger un « parallélisme des formes » en matière de refus et d'acceptation semble donc se rattacher de manière convaincante à l'exigence, bel et bien consacrée par les textes, d'une manifestation de volonté libre¹⁴. Du reste, l'attitude qu'aurait le Conseil d'État, s'il devait connaître d'un recours contre ces sanctions, ne fait guère de doute. Saisi d'un recours contre une première version des lignes directrices de la CNIL en matière de cookies, et alors qu'il n'a pas hésité à en annuler certains aspects, il n'a rien trouvé à redire au passage ici discuté. Il avait estimé, au contraire, que la CNIL qui, en indiquant qu'il devait "être aussi facile de refuser ou de retirer son consentement que de le donner", s'est bornée à caractériser les conditions du refus de l'utilisateur, sans définir de modalités techniques particulières d'expression d'un tel refus, n'a entaché sa délibération d'aucune méconnaissance des règles applicables en la matière » (CE, 19 juin 2020, n° 434684, T., pt 15).

Mais le fait que des responsables de traitement s'accrochent avec l'énergie du désespoir à des bandeaux cookies plus ou moins déloyaux devrait par ailleurs nous amener à réfléchir plus fondamentalement au modèle qui est en train d'être construit. Au moins s'agissant des cookies à pure finalité publicitaire, il n'y a pratiquement aucune bonne raison, à l'échelle d'un utilisateur individuel, de les accepter. Si les grandes entreprises vantent régulièrement le meilleur agrément, pour l'internaute, d'une publicité en lien avec ses centres d'intérêt, ces considérations, à les supposer vraies, sont une faible compensation pour le risque que font courir ces traitements de données personnelles. Les listes de centre d'intérêt peuvent être revendues aux fins de marketing politique ciblé, servir d'appui à des campagnes de propagation de fausses nouvelles, faire tout simplement l'objet de fuites auprès de tiers mal intentionnés. À l'échelle individuelle, pourquoi dire « oui » ? Mais du point de vue de l'entreprise qui finance un service « gratuit » par des publicités personnalisées lucratives, au contraire, c'est le « non » qui n'a pas grand sens. L'internaute ayant refusé les traceurs peut certes être encore exposé à de la publicité non personnalisée, mais le revenu par utilisateur est susceptible de diminuer de façon importante. Dans quel autre secteur de l'industrie ou des services admettrait-on que le prix versé par le client soit à son libre choix ?

Il ne faut voir dans ces lignes aucun plaidoyer en faveur du modèle d'affaires « service gratuit contre publicité ciblée », mais au contraire une incitation à débattre de son existence et de sa réglementation collectivement et politiquement. Renvoyer cette question à de prétendus arbitrages individuels n'a aucun sens¹⁵. Tant que le législateur européen ne se sera pas saisi sérieusement de la question, les responsables de traitement continueront à poser une question qui n'a, à leurs yeux, qu'une seule bonne réponse. C'est la certitude que l'on continuera à biaiser les interfaces aussi longtemps que possible afin que l'erreur ou la paresse entraînent les utilisateurs à donner une réponse qui n'est pas véritablement la leur. C'est abaisser et dévoyer – une fois de plus - la notion de consentement.

Relevons pour finir que l'alternative laissée à l'internaute entre « accepter tous les cookies » et payer un abonnement mensuel n'est, quant à elle, pas prohibée dans son principe¹⁶. Si Google ou

14 La CNIL se rattache aussi, comme les lignes directrices le précisent expressément, à l'art. 7.3 du RGPD, selon lequel « Il est aussi simple de retirer que de donner son consentement ».

15 Notre position sur ces questions est développée dans : « Service en ligne "gratuit" contre publicité ciblée : le modèle d'affaires aux pieds d'argile », Mélanges Storck, Dalloz, 2021 ; « À quoi sert le principe de transparence en droit des données personnelles ? », Dalloz IP/IT, 2020, p.611.

16 Dans une précédente version des lignes directrices, la CNIL avait souhaité prohiber toute forme de « cookie wall », c'est-à-dire d'acceptation obligatoire des cookies pour accéder au service. La formule « cookies ou abonnement payant » en constitue une variante. Dans un arrêt du 19 juin 2020, le Conseil d'État a cependant considéré que « la

Facebook se l'interdisent pour l'heure pour des questions d'image, elle constitue pour l'instant une échappatoire pour la masse des acteurs petits et moyens. Ce modèle va se répandre comme une traînée de poudre. L'attitude de l'internaute, mal éduqué de longue date au « tout gratuit en ligne » et à l'instantanéité, ne fera selon nous guère de doute, et ce quelle que soit la somme demandée : plutôt accepter des traceurs en un instant, au prix de dangers abstraits et lointains, que d'employer argent et énergie en remplissant un formulaire de paiement.

CNIL a[vait] excédé ce qu'elle peut légalement faire, dans le cadre d'un instrument de droit souple ». Il est vrai que les textes en vigueur ne prohibent pas, de manière générale, une telle pratique, ce qui oblige l'autorité à un examen au cas par cas si le consentement des internautes reste libre face à cette alternative.