



HAL
open science

E-Privacy ou la poursuite de la guerre contre la publicité ciblée par d'autres moyens

Emmanuel Netter

► **To cite this version:**

Emmanuel Netter. E-Privacy ou la poursuite de la guerre contre la publicité ciblée par d'autres moyens. Dalloz IP/IT : droit de la propriété intellectuelle et du numérique, 2021, 04 et 02, pp.226. halshs-03218360

HAL Id: halshs-03218360

<https://shs.hal.science/halshs-03218360>

Submitted on 15 Jul 2021

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.

E-privacy ou la poursuite de la guerre contre la publicité ciblée par d'autres moyens

*Emmanuel Netter, professeur de droit privé à l'université d'Avignon
LBNC (EA3788)*

Dalloz IP / IT 2021, p. 226

Par sa délibération du 7 décembre 2020, la CNIL condamne des sociétés du groupe Alphabet à une sanction de 100 millions d'euros : 60 millions pour la maison-mère américaine Google LLC, 40 millions pour la tête de pont européenne Google Ireland Limited (ci-après GIL), pour avoir manqué à leurs obligations en matière de dépôt de cookies sur les terminaux des utilisateurs. Une décision du même jour prononce une sanction de 35 millions d'euros « seulement » contre Amazon Europe, pour des motifs quasiment identiques (SAN 2020-013).

Nous avons commenté dans ces mêmes colonnes une délibération « Android » de 2019, infligeant déjà à Google une amende de 50 millions d'euros, ce qui constituait alors un record historique (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 ; elle fut confirmée en tous points par Conseil d'État, 12 juin 2020, n° 430810). L'autorité s'y appuyait sur le RGPD, ce qu'elle ne peut plus faire aujourd'hui face aux principaux géants du numérique, pour des raisons sur lesquelles nous reviendrons. On y trouvait exactement les mêmes ingrédients qu'aujourd'hui : en préambule, une lutte acharnée autour de la compétence territoriale de la CNIL (I) ; sur le fond, une conception rigoureuse de l'information et du consentement des personnes concernées (III) ; dans l'ensemble, une décision qui fait peser de lourdes menaces sur des centaines de responsables de traitement dont le financement repose en tout ou partie sur de la publicité personnalisée (IV). La délibération rapportée ajoute toutefois une question nouvelle, relative à la co-responsabilité de traitement (II).

I – La compétence : avec e-privacy, la fermeture du guichet unique

À l'époque de la décision Android, nous avons expliqué que si d'autres grands acteurs du numérique ne s'étaient pas trouvés épinglés au tableau de chasse de la CNIL en même temps que Google, cela s'expliquait moins par leurs vertus supérieures que par leur célérité à trouver refuge en Irlande. Le RGPD prévoit en effet un mécanisme de « guichet unique », qui dans le cas de l'Irlande, porte admirablement son nom anglais de « one-stop-shop » : on s'y arrête pour ne plus jamais se mouvoir. Depuis l'entrée en application du règlement et jusqu'ici, le *Data Protection Commissioner* de Dublin a fait la démonstration constante de son incapacité à faire aboutir les gigantesques dossiers dont il est saisi – en particulier celui qui oppose None of Your Business, l'association menée par Max Shrems, à Facebook. Si une timide sanction contre Twitter a été prononcée récemment, c'est après que le projet de sanction irlandais ait été mis en minorité par les autres autorités européennes, au sein du Comité européen de la Protection des données (CEPD), dans le cadre de la procédure de règlement des litiges de l'article 65 du règlement (CEPD, Decision

01/2020 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Twitter International Company under Article 65(1)(a) GDPR).

Dans l'affaire Android, la CNIL avait opportunément tiré partie des pouvoirs insuffisants conférés par Google à son établissement irlandais pour considérer que la société n'avait « pas d'établissement principal en Europe ». Moyennant une interprétation du règlement qui nous avait semblé pour le moins audacieuse, mais à laquelle le Conseil d'État n'a rien trouvé à redire, la CNIL avait pu fonder sa compétence territoriale et agir seule. Depuis, le géant de Mountain View a tiré les leçons de ses erreurs et entonné, avec nombre de ses camarades de la Silicon Valley, l'air entraînant de « Dublin can be heaven ».

Cela a depuis été écrit régulièrement, sous des formes diverses : le guichet unique est une machine à faire sauter le RGPD. En présentant récemment son projet de *Digital Services Act*, la Commission européenne a d'ailleurs pris soin de se réserver une faculté d'initier elle-même des poursuites contre les grandes plateformes, pour le cas où l'autorité chef de file apparaîtrait défaillante (art. 51).

Ceux qui pensaient la CNIL totalement désarmée avaient cependant oublié l'existence de la directive e-privacy (2002/58/CE), texte sectoriel qui régit la collecte de données personnelles en matière de communications électroniques, et qui s'applique donc en particulier au dépôt et à la lecture d'informations sur les terminaux des utilisateurs : ce que l'on a coutume d'appeler les « cookies ». Coup de théâtre : l'autorité, que certains prétendent velléitaire, revient par la fenêtre après avoir été chassée par la porte. Car en effet, la directive e-privacy ne prévoit pas de mécanisme de guichet unique.

Les sociétés Google avancent cependant que « le spécial déroge au général » (§26) : puisqu'il existe des règles relatives au chef de file dans le RGPD mais que e-privacy est muet sur un tel mécanisme de coopération, le guichet unique devrait l'emporter. Mais l'autorité reprend aussitôt l'adage à son profit : les fondements de licéité admissibles en matière de cookies sont plus étroits que ceux offerts par l'article 6 du RGPD, puisque e-privacy requiert nécessairement un consentement. La directive, plus spéciale, déroge donc au règlement sur ce point ; or, cette directive renvoie aux États le soin de fixer les règles relatives à la compétence territoriale (§29).

Mais le passage qui emporte véritablement la conviction, nous semble-t-il, figure au §32. La CNIL y relève que la directive e-privacy offre aux États le choix de faire superviser l'application du texte par leur autorité de protection des données **ou bien** par leur autorité de régulation des télécommunications (l'équivalent de notre ARCEP). Dès lors, les mécanismes de coopération du RGPD sont inapplicables, puisqu'ils s'appuient à plusieurs reprises sur la réunion de toutes les CNILs européennes au sein d'une enceinte, le CEPD. Or, les homologues de l'ARCEP n'ont pas de siège au CEPD. Le one-stop-shop est donc bien inapplicable dans le cadre de e-privacy.

D'autres arguments sont encore avancés en ce sens, même s'ils paraissent alors superfétatoires, comme les débats autour de l'opportunité d'insérer un mécanisme de guichet unique dans le projet de règlement e-privacy, en discussion depuis trois ans, et qui a vocation à remplacer la directive. Si on hésite à introduire cette nouveauté, explique la CNIL, c'est bien qu'elle diffère de l'existant (§34).

Le one-stop-shop ayant été évincé, il reste à fonder positivement la compétence territoriale de l'autorité française. E-Privacy ne fournissant pas directement la solution, elle est à rechercher dans

le droit interne français, en l'occurrence l'article 3 de la loi informatique et libertés. Sous réserve des dispositions du RGPD (dont on a vu qu'elles n'étaient pas applicables ici), « l'ensemble des dispositions de la présente loi s'appliquent aux traitements des données à caractère personnel effectués **dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire français (...)** ». En l'espèce, le responsable de traitement dispose, avec Google France, d'un établissement sur le territoire français.

II – Les responsables : maison-mère américaine et filiale irlandaise conjointement

Mais qui, au juste, est ce responsable de traitement ? GIL estimait revêtir seule cette qualité. La CNIL décide au contraire que GIL et Google LLC sont conjointement responsables du traitement. L'enjeu est clair : une telle qualification permet de sanctionner les deux sociétés, chacune sur la base de son chiffre d'affaires annuel. En raison des renvois opérés par la directive e-privacy, les définitions à manier ici sont celles du RGPD. Est un responsable de traitement celui qui participe « à la définition des moyens et des finalités » du traitement (art. 4,7). Plusieurs personnes peuvent prendre ces décisions conjointement (art. 26, 1).

Que GIL soit responsable de traitement ne faisait guère de doute : les deux sociétés avaient elles-mêmes indiqué que la filiale irlandaise « applique, par exemple, des durées de conservation des cookies plus courtes par rapport à d'autres régions du monde et qu'elle limite l'étendue des traitements liés à la personnalisation de la publicité en Europe par rapport au reste du monde. [Elle] n'utilise pas certaines catégories de données pour effectuer de la publicité personnalisée telles que les ressources du foyer supposées. La société GIL ne met pas en place de publicité personnalisée pour les enfants dont elle suppose qu'ils sont mineurs au sens du RGPD » (§56). GIL prenait donc des décisions pour adapter les produits Google aux caractéristiques et à la réglementation du marché européen, ce qui est bien une façon de modeler le traitement. Relevons que ce pouvoir décisionnel fort de l'Irlande est précisément ce qui avait manqué, à l'époque de la décision Android, pour que Google puisse opposer à la CNIL le one-stop-shop, dans une matière qui relevait alors du RGPD.

Mais ensuite, la CNIL relève à juste titre que les outils que GIL ne fait qu'adapter à la marge sont conçus et développés par Google LLC, en particulier les cookies dont le dépôt sur les terminaux français est à l'origine de l'affaire (§59). De surcroît, Google LLC « est représentée dans les organes adoptant les décisions relatives au déploiement des produits au sein de l'EEE et en Suisse » (§61). L'autorité française ne peut s'empêcher de noter par ailleurs que le DPO de la filiale irlandaise se trouve... en Californie, afin d'être « au plus près des décideurs de l'entreprise » (§62).

Lorsque l'on connaît la jurisprudence « Fashion ID » de la CJUE (29 juillet 2019, C-40-17), selon laquelle la simple insertion d'un bouton « j'aime » Facebook dans une page web fait de l'éditeur de la page un co-responsable de traitement, la solution adoptée ici par la CNIL ne surprend pas. Cette jurisprudence européenne avait bien précisé qu'il n'est pas nécessaire que deux acteurs aient une responsabilité équivalente dans la conception des moyens et finalités du traitement pour être jugés co-responsables au sens du RGPD : il suffit qu'ils y participent tous les deux, ce qui est bien le cas en l'espèce des deux sociétés Google.

Il est intéressant de relever que les deux sociétés avaient conclu un contrat plaçant Google LLC en position de sous-traitant, mais que la CNIL ne s'est pas arrêtée à l'intitulé de l'acte : analysant la réalité de la relation sous-jacente, elle lui a restitué sa juste qualification. L'artifice n'a pas résisté.

III – Le fond : une recette pour des cookies réussis

Par comparaison avec la bataille acharnée qui précède pour fonder la compétence territoriale de la CNIL et déterminer les responsables, le fond de la décision est simple et se comprend aisément. En substance, trois reproches étaient formulés s'agissant des cookies utilisés par Google lorsqu'un internaute utilise son moteur de recherche généraliste : une information insuffisante (logiquement suivie d'un consentement creux), un dépôt trop précoce des fichiers dans les terminaux, un mécanisme d'opposition défaillant. Ce sont autant de manquements aux exigences de l'article 82 de la loi informatique et libertés, qui constitue la transposition des exigences de e-privacy en droit français.

De même que la sanction Android avait fourni à la CNIL l'occasion d'envoyer un certain nombre de messages *urbi et orbi*, ce passage de la décision constitue un avertissement solennel à tous les responsables de traitement faisant usage de cookies. Une fois de plus, ceux qui imaginent qu'une telle sanction ne concerne que les « GAFA » commettent une grave erreur.

Il est d'abord reproché aux sociétés Google de ne pas avoir informé correctement les internautes. Les reproches formulés ici ne sont pas sans rappeler ceux adressés à la politique de confidentialité de Google dans l'affaire Android : obscurité, complexité. Google estime une fois de plus avoir conçu une information par étapes, par strates, permettant au lecteur d'en dévoiler les éléments de manière douce et progressive. La CNIL rétorque que l'internaute, à moins de perdre un temps et une énergie dont il ne dispose jamais, ne comprend pas les finalités des traitements de données, et ne s'aperçoit pas qu'il peut s'opposer au dépôt de cookies. Au cours de la procédure ouverte contre elles, les sociétés ont proposé une nouvelle version du bandeau cookies, qui n'a toujours pas convaincu l'autorité française. Chacun pourra en faire l'expérience : en janvier 2021, on rencontre encore un premier écran assez flou qui propose « plus d'informations » ; puis, au pied d'un second texte très riche en précisions, un bouton « autres options » renvoie à une série d'outils de gestion de la confidentialité, chacun étant assorti d'un descriptif. On ne voit aucune façon véritablement rapide et efficace de choisir quels cookies seront déposés, voire de procéder à un rejet en bloc de tous les cookies non indispensables au fonctionnement du service, comme c'est le cas sur les sites adoptant les meilleures pratiques. Dans ces conditions, on ne voit pas comment considérer que l'information délivrée est suffisamment « claire » et que le consentement des internautes a une signification véritable, au-delà d'une envie de se débarrasser au plus vite d'une « fenêtre surgissante » agaçante pour accéder au service.

De manière plus indiscutable encore, il était reproché à Google de déposer pas moins de sept cookies, dont quatre à finalité publicitaire, dès la connexion de l'internaute, et avant tout choix de sa part. Ces manquements ont été reconnus. À la date de la décision, ils étaient corrigés.

Enfin, la CNIL expose avoir suivi lors de son contrôle en ligne la procédure d'*opt-out*, supposée désactiver entièrement la personnalisation des annonces, et avoir pourtant constaté la présence d'un cookie non-essentiel sur le terminal utilisé.

Les réticences des sociétés Google à produire un bandeau cookie plus simple ne s'expliquent évidemment pas par leur amateurisme : elles disposent d'ingénieurs et de juristes du plus haut niveau. Une fois de plus, c'est tout simplement un modèle d'affaires qui est en jeu.

IV– Le résultat : une pression encore accrue sur la publicité ciblée

Pourquoi Google, dans l'affaire Android, avait-il pré-coché les cases relatives aux traitements nécessaires à la publicité ciblée ? Pourquoi rend-il, au cas d'espèce, la finalité des cookies si difficile à saisir, le refus de leur dépôt si compliqué ? La réponse était et demeure extrêmement simple : s'il est possible de profiter d'un service « gratuit » en ayant le choix de voir ou non ses centres d'intérêts découpés en tranches pour être vendus au plus offrant, la plupart des internautes voudront évidemment le beurre (le service) et l'argent du beurre (l'absence d'exposition de leurs données personnelles). L'option proposée n'a guère de sens. Nous l'avons souvent écrit : en refusant de réglementer de manière directe, pour l'interdire ou l'encadrer, ce modèle d'affaires si particulier, les législateurs français et européen ont transformé ce qui devrait être un choix collectif et politique en une multitude d'arbitrages individuels totalement absurdes (V. « À quoi sert le principe de transparence en droit des données personnelles ? », Dalloz IP/IT, novembre 2020, p. 611). Les politiques de confidentialité qui tergiversent, les parcours d'inscription chantournés et les *dark patterns* sont autant de corollaires de ce système vicié : lorsqu'ils recueillent des consentements, les « publicitaires » ne veulent pas connaître votre opinion véritable. Ils veulent que cette réponse soit « oui », car il en va de leur survie. Alors même qu'aucun texte n'interdit expressément de financer un service en ligne par de la publicité ciblée, nous pronostiquions que la CNIL allait peu à peu tirer des conséquences de dispositions du RGPD et de e-privacy, dans des décisions d'apparence faussement technique, pour aboutir à une interdiction de fait de ce modèle d'affaires (V. « Service en ligne gratuit contre publicité ciblée : le modèle d'affaires aux pieds d'argile », in Mélanges Storck, à paraître, Dalloz, février 2021). La décision rapportée s'inscrit parfaitement dans cette perspective.