Sanction à 50 millions d'euros : au-delà de Google, la CNIL s'attaque aux politiques de confidentialité obscures et aux consentements creux

Emmanuel Netter

▶ **To cite this version:**

Emmanuel Netter. Sanction à 50 millions d'euros : au-delà de Google, la CNIL s'attaque aux politiques de confidentialité obscures et aux consentements creux. Dalloz IP/IT : droit de la propriété intellectuelle et du numérique, 2019, 3, pp.165. hal-02314524

HAL Id: hal-02314524
https://hal.science/hal-02314524

Submitted on 12 Oct 2019

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.

CNIL, délibération n° SAN-2019-001 du 21 janvier 2019
Commentaire par Emmanuel Netter, maître de conférences HDR à l'Université d'Avignon, Laboratoire Biens, normes, contrats (EA 3788).

Le RGPD à peine entré en vigueur, les associations La Quadrature du Net (LQN) et None of Your Business (NYB) ont déposé auprès de la CNIL, les 25 et 28 mai derniers, des plaintes collectives contre plusieurs grandes sociétés de l'économie numérique, dont Google. De nombreux manquements étaient allégués, qui ne pouvaient tous être traités d'un bloc. La délibération du 21 janvier 2019 n'est donc que la première d'une série à venir, mais elle suscitait des attentes particulières. Il était évident qu'elle aurait valeur de test, et qu'à cette aune on mesurerait la capacité des autorités nationales de contrôle à imposer, sur le terrain, une lecture exigeante du RGPD. La CNIL ne s'est pas dérobée. Après un délai d'instruction serré, elle rend une décision de sanction dont on aurait tort de retenir seulement qui elle vise et quel est son montant – 50 millions d'euros (Commentaire : O. Tambou, « Décryptage autour de la première condamnation de Google par la CNIL post-RGPD », Dalloz actu. du 30 janvier 2019). La délibération déborde de messages adressés à tous les responsables de traitement, et fixe la doctrine de l'autorité sur plusieurs points d'une importance cruciale. Elle concerne l'entrée dans l'univers de services de Google, suite à l'acquisition d'un appareil sous système d'exploitation Android et à la création d'un compte utilisateur.

Passons sur l'examen de la recevabilité des plaintes collectives portées par LQN et NYB : la CNIL ayant rappelé qu'elle peut s'auto-saisir chaque fois que ses services ont constaté des manquements au règlement, l'enjeu était très limité. Pour le surplus, trois grandes questions sont abordées : la compétence de l'autorité française pour juger d'un traitement transfrontalier alors qu'elle se prononce seule ; l'exigence de clarté et d'accessibilité des politiques de confidentialité ; l'exigence d'un fondement de licéité pour le traitement dans le contexte d'une exposition de l'internaute à des annonces personnalisées.

La compétence de la CNIL : diviser pour seule régner

La première des trois grandes parties de la décision vise à fonder la compétence, à l'égard du traitement de données considéré, de la CNIL agissant seule. Il fallait pour cela que l'autorité française justifie l'éviction du mécanisme dit de « guichet unique », qui vise à confier la conduite des procédures intéressant plusieurs États membres à une « autorité chef de file ». La société Google exigeait au contraire que le *Data Protection Commissionner* irlandais prenne la main sur ce dossier. La CNIL n'aurait pas été évincée pour autant, mais le DPC aurait été en mesure d'imposer au dossier sa vision, et surtout son tempo : c'est le destin qui attend notamment le dossier « Facebook ». Or, si l'Irlande a tout fait pour devenir le havre européen des grandes sociétés de la Silicon Valley, elle a malencontreusement oublié d'en tirer les conséquences en dotant son autorité de protection des données des moyens correspondants : l'enlisement était donc à craindre. À la lumière de ces éléments, on comprend mieux l'interprétation volontariste que l'autorité française a tenté d'imprimer à des articles du RGPD dont la clarté n'est pas la qualité première.

Le texte autour duquel est bâti le mécanisme d'autorité chef de file est l'article 56 du règlement. Sa construction générale semble d'abord favorable à Google : le premier point requiert qu'un chef de file soit désigné lorsque le traitement est « transfrontalier ». Son deuxième point pose une exception : chaque autorité nationale sera compétente face à une réclamation ou une violation du règlement qui « concerne uniquement un établissement dans l'État membre dont elle relève ou affecte sensiblement des personnes concernées dans cet État membre uniquement » : à difficultés locales, solutions locales. Or, les questions posées dans ce dossier le sont bien à l'échelle de l'Europe entière. À ce stade, on doute encore que la CNIL puisse agir en franc-tireur.

Supposons cependant qu'un chef de file doive être désigné. Qui cela doit-il être ? L'article 56 répond : « l'autorité de contrôle de **l'établissement principal** ou de l'établissement unique du responsable du traitement » (les caractères gras dans les citations sont toujours de notre fait). La question rebondit : qu'est-ce qu'un établissement principal ? Toutes les définitions du RGPD figurent à l'article 4, et en son point 16 on trouve celle de l'établissement principal : « en ce qui concerne un responsable du traitement établi dans plusieurs États membres, **le lieu de son administration centrale** dans l'Union, **à moins que** les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement a le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal ». Formulons ici une observation importante : si le règlement envisage l'hypothèse d'une discordance entre le lieu où se situe l'administration centrale et celui où l'on prend les décisions relatives aux traitements (pour donner alors la priorité à ce dernier), cela signifie nécessairement que l'administration centrale ne se définit pas comme le lieu où l'on prend de telles décisions.

Pour comprendre l'interprétation mobilisée par la CNIL, il faut enfin citer le considérant 36 du règlement : « L'établissement principal (...) devrait supposer l'exercice effectif et réel **d'activités de gestion déterminant les décisions principales** quant aux finalités et aux moyens du traitement dans le cadre d'un dispositif stable ».

L'établissement principal est donc un lieu où s'exercent des activités de gestion, ce qui semble être le cas de Google Irlande, qui centralise notamment les opérations de comptabilité ou les conclusions de contrats publicitaires à l'échelle européenne. Mais ces activités de gestion doivent « déterminer » les décisions relatives aux finalités et moyens du traitement, formule particulièrement obscure dont on peine à cerner le sens. La CNIL s'engouffre aussitôt dans la brèche et affirme que « pour pouvoir être qualifié d'établissement principal, l'établissement concerné **doit disposer d'un pouvoir de décision** vis-à-vis des traitements de données », ce qui n'est pas tout à fait la même chose. Ce pouvoir de décision était situé pour Google aux USA, à la date du constat opéré par la CNIL (Depuis, Google LLC a transféré des pouvoirs décisionnels concernant le traitement à son établissement irlandais, ce qui pourrait modifier la solution s'agissant des violations du règlement constatées après cette date). Il n'y a aucun établissement principal en Europe ; il n'y a donc pas besoin de chef de file ; les autorités nationales sont donc libres de toute obligation de se coordonner. La décision est cohérente avec les lignes directrices du G29 (Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant, 5 avril 2017, p. 6 : « Conformément à l'approche ressortant du règlement général, l'administration centrale dans l'Union est le lieu où sont prises les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel, et ce lieu a le pouvoir de faire appliquer ces décisions »). Elle est conforme à une prise de position publique du DPC qui, dans la presse, a affirmé ne pas se considérer comme le régulateur principal de Google (V. l'article de l'Irish Times cité par la CNIL dans sa délibération). Elle n'a pas dérangé le Comité européen pour la protection des données qui, prévenu par la CNIL, est resté inerte (La CNIL précise avoir communiqué les réclamations aux autres autorités, et relève qu'ensuite « aucune autorité de contrôle, ni le Président du Comité, n'ont jugé nécessaire de saisir le CEPD en raison d'incertitudes sur l'identification de l'autorité chef de file ou la compétence de la CNIL »). Pour autant, elle n'est pas incontestable au regard du règlement : la lettre obscure d'un considérant prévaut ici sur l'esprit de l'article 56, qui est : à problèmes européens, solutions européennes. Du point de vue de l'opportunité, elle n'est pas non plus totalement satisfaisante. Dans toutes les hypothèses où des sociétés américaines n'ont pas transféré un pouvoir de décision net et fort sur le sol européen en matière de traitements, et alors même que leur administration serait bel et bien coordonnée sur notre sol, il y aura potentiellement 28 procédures menées contre elles. Ces sociétés ne seront pas seules à

en pâtir. Un jour viendra où des questions strictement identiques recevront des réponses contradictoires à travers l'Europe. On regrettera peut-être, alors, que les différences de points de vue entre régulateurs européens n'aient pas été réduites dans le secret de délibérations internes, plutôt qu'en place publique.

La transparence : dans le labyrinthe des politiques de confidentialité

La deuxième grande question abordée par la délibération est celle du respect des obligations de transparence, qui pèsent sur le responsable de traitement au bénéfice des personnes concernées, et qui sont régies notamment par les articles 12 et 13 du règlement.

L'article 12 exige en particulier que le responsable de traitement fournisse aux personnes dont les données sont traitées un certain nombre d'informations « (…) d'une façon concise, transparente, **compréhensible et aisément accessible**, en des termes **clairs et simples** (...) ». Nombreux sont ceux qui ont souri à la lecture de ce texte, mesurant l'abîme qui sépare actuellement cet idéal de la réalité des politiques de confidentialité. Mais peut-être le temps des sarcasmes sera-t-il bientôt révolu ? La CNIL affiche ici sans ambiguïté son intention de donner vie à ce texte, de lui conférer un plein effet. Prétexte est pris des activités d'un des plus gros responsables de traitement, mais qu'on ne s'y trompe pas : le message s'adresse à tous. Contemplant la politique de confidentialité de Google, et à travers elle toutes les autres, le régulateur français lui adresse en substance deux reproches majeurs : sa construction même, ainsi que sa formulation.

Dans un premier temps, c'est la construction, l'architecture, le design de la politique de confidentialité qui est envisagée. Le document de Google requiert d'ouvrir des tiroirs ou de dérouler des accordéons ; il exige de cliquer régulièrement sur « plus d'informations » ou de demander « davantage de détails ». Le monument ne se laisse pas embrasser d'un coup d'œil, mais se visite par étapes. Google faisait valoir que scinder l'information en petites unités plus digestes plutôt que d'écraser le lecteur sous un immense monolithe, c'est servir l'intelligibilité et non la trahir. La CNIL ne condamne pas le procédé dans son principe, mais l'attaque au cas d'espèce pour ses modalités concrètes. Prenant plusieurs exemples d'informations importantes - les types d'informations exploités pour la publicité ciblée, les explications relatives à la géolocalisation ou encore les durées de conservation -, elle relate pour chacune le nombre d'actions nécessaires à son appréhension complète, et en déduit que c'est là trop demander à un utilisateur ordinaire. La démonstration est convaincante. Elle repose cependant sur des appréciations très factuelles, qu'il eût été utile que les autorités européennes mènent ensemble, le risque étant sans cela qu'un même nombre de clics attendu du lecteur soit jugé épuisant à Paris et raisonnable à Madrid.

Les rédacteurs de politiques de confidentialité relatives à des traitements très complexes sont ainsi placés devant un exercice difficile, qui suppose d'aérer le document pour ne pas assommer, tout en lui conservant sa cohérence pour ne pas égarer. Les exigences de forme sont si contraignantes qu'elle se muent insensiblement en exigences de fond. En effet, au-delà d'un certain degré de sophistication du traitement, le responsable n'est-il pas face à l'impossibilité radicale de l'expliquer « en termes clairs et simples » ? L'idée n'est pas absurde. Elle ne date pas du RGPD, mais elle a quarante ans : si vous n'êtes pas capable d'expliquer aux individus ce que vous faites avec leurs données, alors vous devriez vous arrêter. Ce qui est certain, par ailleurs, c'est que plus les traitements sont intrusifs, plus la CNIL attendra du responsable qu'il déploie des trésors de pédagogie. Ce point est souligné à plusieurs reprises.

Dans un deuxième temps, la CNIL envisage non plus l'architecture générale du document, mais certaines formulations qui lui paraissent être excessivement floues. Ainsi, à propos des données collectées, le premier niveau de la politique de confidentialité, celui auquel on accède sans avoir à accomplir d'action supplémentaire, précise : « **Il peut s'agir d'informations (…) plus complexes**,

comme les annonces que vous trouvez les plus utiles, les personnes qui vous intéressent le plus sur le Web ou les vidéos YouTube qui sont susceptibles de vous plaire ». L'intitulé de la catégorie est pour le moins fuyant, et il est suivi de simples exemples. Plus loin, au titre des durées de conservation, apparaît une catégorie « Informations conservées pendant de longues périodes pour des raisons précises », mais la CNIL n'a trouvé ensuite que des explications très générales sur les finalités correspondantes, sans indication des critères permettant de déterminer quand les données seront finalement supprimées.

Google n'est pas la seule société à s'exposer à de telles critiques. La politique de confidentialité de Facebook en constitue un exemple intéressant. Tout d'abord, elle aussi est à tiroirs. Au sein de la longue page consacrée aux usages des données, des pages spéciales s'ouvrent si l'on veut comprendre la politique en matière de publicité - celle-ci est presque un site à elle seule - ou de reconnaissance faciale. Elle contient elle aussi, ensuite, des formules particulièrement imprécises. S'agissant des usages par les tiers, on lit : « Nous fournissons des statistiques et des informations (insights) agrégées qui permettent aux individus et aux entreprises de comprendre la façon dont les gens interagissent avec leurs publications, leurs annonces, leurs Pages, leurs vidéos et tout autre contenu sur les Produits Facebook et en dehors ». Il est difficile de faire plus vague. Un peu plus loin, on rencontre encore : « Nous donnons **des informations et du contenu aux fournisseurs et prestataires de services qui soutiennent nos activités**, notamment en proposant des services d'infrastructure technique, en analysant l'utilisation de nos Produits, en fournissant un service à la clientèle, en facilitant les processus de paiement ou en réalisant des sondages ».

Ces structures trop éclatées, ces formules trop évanescentes sont-elles le résultat d'une saine volonté de simplifier ayant seulement dégénéré par excès ? Ou bien constituent-elles la manifestation d'un désir parfaitement conscient, maîtrisé, d'endormir la vigilance du lecteur ? La pédagogie est parfois le masque facile de la dissimulation. Sans préjuger des mobiles animant les rédacteurs, la CNIL lance en somme un avertissement : plus de documents lénifiants. Lorsque l'on réserve à l'intimité des personnes des traitements d'une grande puissance, il vaut mieux les inquiéter trop que pas assez, et leur en dire trop que trop peu. Au moment de rédiger ces politiques, le service marketing doit relâcher son emprise sur la plume et le service juridique l'affermir.

Disons-le sans détour : aujourd'hui, rares sont les responsables de traitement qui satisfont aux critères ainsi posés par la CNIL, tout du moins s'agissant des grands services en ligne. Le défi que leur lance l'autorité française dans la seconde partie de sa décision est difficile, mais il n'est pas insurmontable. Il en va peut-être autrement de la troisième partie, qui fera souffler un vent de panique dans le monde de la publicité ciblée.

Le fondement de licéité : qui ne dit mot ne consent pas

Un traitement de données à caractère personnel n'est permis que si le responsable peut se prévaloir de l'un des fondements de licéité figurant dans la liste limitative de l'article 6 du RGPD. On y trouve notamment : « la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques » ; « le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie (...) » ; « le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée (...) ».

« L'intérêt légitime » du responsable de traitement doit être invoqué avec une grande prudence, car il requiert une mise en balance avec les droits de la personne concernée. Les résultats d'une telle pesée ne sont pas faciles à prévoir, et les analyses de la CNIL peuvent diverger de celles du responsable de traitement au moment du contrôle, et il est alors trop tard : la société Google l'avait appris à ses dépens il y a quatre ans (Délibération n°2013-420 du 3 janvier 2014). Aussi

n'invoquait-elle ce fondement de licéité que pour l'affichage de publicités « peu ciblées », pourrait-on dire, en ce qu'elles reposaient non pas sur la connaissance précise des centres d'intérêt de l'utilisateur, mais seulement sur le contexte de navigation.

En revanche, la publicité véritablement individualisée était fondée sur le consentement de la personne au traitement de ses données. Pour la CNIL, cela implique deux choses. Premièrement, que l'on comprenne ce à quoi on consent, ce qui renvoie à la partie de sa décision consacrée à l'intelligibilité de la politique de confidentialité. Deuxièmement, que le consentement se donne à voir par « un acte positif clair », pour reprendre les termes de l'article 4,11° du règlement.

Rédiger de belles politiques de confidentialité ou de beaux contrats ne sert à rien si personne ne les lit. Cette réalité crue n'a pas attendu le droit des données personnelles pour se faire connaître des juristes. Pour ralentir la course folle vers un consentement mécanique et vide de signification, le législateur fait assaut d'imagination : un exemple bien connu - et à ne pas suivre - est celui des mentions manuscrites laborieusement recopiées par les cautions, supposées les pénétrer du sens de leur engagement tandis que les minutes s'écoulent. En ligne plus encore qu'ailleurs, l'utilisateur a tendance à foncer comme un taureau furieux vers l'instant où il pourra bénéficier du service. Il faut le freiner dans son élan pour l'obliger à réfléchir : l'exigence d'un consentement exprimé par un acte positif clair le permet.

La société Google avait joué avec les limites, dans la conception de son parcours utilisateur. Elle demandait aux utilisateurs d'accepter un ensemble de traitements en un seul clic, incluant celui destiné à afficher des publicités ciblées. Une « fenêtre surgissante » avertissait alors l'utilisateur que cela impliquait des annonces personnalisées : il lui était alors loisible de cliquer sur « plus d'options » et là, seulement, il pouvait refuser la publicité ciblée. Ce système est certes meilleur que ce que proposent la plupart des services en ligne, avec un seul gros bouton d'acceptation qui n'est suivi d'aucun avertissement, ou bien la nécessité de décocher un par un les transferts vers des dizaines de régies publicitaires. En somme, c'est une variété subtile d'*opt-out* que proposait Google, mais c'est bien un *opt-in* qu'exige le règlement. Intransigeante sur ce point, la CNIL est fidèle au texte.

Pour avoir une vision complète du résultat, il faut citer l'article 7, 4° du RGPD : « Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat ». En d'autres termes, Google doit prévoir un parcours utilisateur qui mène, s'il est suivi en ligne droite, à un service parfaitement fonctionnel sans aucune publicité ciblée. Pour que l'on recherche ses centres d'intérêt afin de lui fournir des annonces personnalisées, celui qui ouvre un compte devra le demander activement, alors même qu'il n'y trouvera aucun avantage particulier. En rester là reviendrait à mettre à mort le modèle d'affaires « service gratuit contre publicité ciblée ».

Le mot « gratuit » doit ici s'entendre comme « sans contrepartie monétaire », car il s'agit bien de contrats synallagmatiques, dans lesquels la contrepartie fournie par l'utilisateur n'est versée ni en euros, ni en dollars, mais en fragments d'intimité (V. not. J. Rochfeld, « Le « contrat de fourniture de contenus numériques » : la reconnaissance de l'économie spécifique « contenus contre données » », Dalloz IP/IT, 2017, p. 15). N'y a-t-il pas là une piste à suivre ? Parmi les fondements de licéité alternatifs au consentement, on trouvait : « le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ». Dans les contrats classiques, pour lesquels le client règle en monnaie, ces traitements sont nécessaires à l'exécution de la prestation du professionnel : il doit par exemple collecter une adresse s'il doit y effectuer une livraison. On a beaucoup moins envisagé que le traitement soit nécessaire à la fourniture de la prestation du client, mais n'est-ce pas le cas

s'il a promis de s'exposer à des publicités ? La question est à l'étude au sein du CEPD (L'agenda de la sixième réunion plénière mentionne « Position Paper on reliance on Art. 6.1 b GDPR in context of "free" online services » : http://edpb.europa.eu/our-work-tools/our-documents/agenda-meetings/agenda-sixth-plenary_en).

Le recours à ce fondement de licéité constitue donc une piste intéressante toutes les fois où il y a création d'un compte, et donc conclusion d'un contrat (tel n'est pas le cas, par exemple, lorsqu'un internaute visite le site internet d'un journal et y est exposé à de la publicité ciblée sans avoir conclu aucune convention). Un problème potentiel subsiste : si le service souscrit n'a aucun concurrent sérieux, comme Facebook, ou que tous les concurrents fonctionnent sur un modèle de pseudo-gratuité, le client n'a pas véritablement le choix, et son consentement au contrat incluant des annonces personnalisées peut apparaître contraint. L'avenir est peut-être alors à des offres hybrides, comme celle du Washington Post : une offre pseudo-gratuite ou à coût faible, associée à de la publicité ciblée, et une offre à plein tarif sans aucun traitement de données aux fins d'afficher des annonces personnalisées. L'ensemble suppose des politiques de confidentialité parfaitement explicites, qui permettront aux utilisateurs de décider en pleine conscience.

Il est certes également possible de ne tolérer, à l'avenir, que des publicités non ciblées, fondées sur l'intérêt légitime du responsable de traitement. Mais le revenu par utilisateur ne sera pas le même, et certains services actuellement financés par des annonces personnalisées seront revus à la baisse ou disparaîtront. Avec cette délibération de la CNIL, c'est un très important débat qui est implicitement lancé.

La sanction

L'amende administrative de 50 millions d'euros infligée à Google est-elle proportionnée ? Il est difficile de répondre à cette question. D'abord, parce que les plaintes collectives adressées à la CNIL visent de multiples services de cette société, de sorte que plusieurs autres décisions seront rendues en France. Cela, on ne pouvait l'éviter. Mais ensuite, parce que l'approche solitaire de l'autorité française ouvre la voie, pour chaque service contrevenant au règlement, à 28 décisions nationales possibles, chacune proportionnant sa sanction locale à l'ampleur de la population utilisatrice. Vingt, cinquante ou peut-être cent décisions peuvent donc être rendues contre cette société dans un proche avenir. Or, on ne pourra véritablement juger de la juste proportion de la punition qu'en cumulant toutes les amendes prononcées localement. Que faire, dans quelques mois ou années, si le total apparaît excessif ? Qui sera en mesure d'en juger ? Quelle correction pourra-t-on apporter ? Faut-il, appliquant une règle de trois aux populations respectives de la France et de l'Union, considérer d'ores et déjà qu'un total de 380 millions euros d'amendes au moins est encouru pour ce seul dossier ? Mais de nombreux pays pourraient ne jamais engager de poursuites (Il existe des « Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement 2016/679 », adoptées le 3 octobre 2017, mais elles ne paraissent pas répondre à ces questions.). Le considérant 150 du règlement encourage les autorités, à défaut de désignation d'un chef de file, à débattre ensemble du montant des sanctions à infliger, dans le cadre du mécanisme de « cohérence ». La décision de la CNIL n'indique pas si ce débat a eu lieu en l'espèce, et on peut le regretter.

PERSPECTIVES

Les louanges et les réserves qu'appelle la décision ont une origine commune : le fort volontarisme qu'affiche ici la CNIL. Ce volontarisme construit : la crédibilité de l'autorité française sur la scène post-RGPD ; une vision exigeante de la transparence et du consentement au traitement des données. Il détruit, ou du moins bouscule : un certain idéal de coopération entre autorités européennes ; le modèle d'affaires dominant en ligne, celui des services pseudo-gratuits contre l'exposition à de la

publicité ciblée. Il est rare qu'une décision mérite qu'on la qualifie « d'historique », sans que ce terme soit en rien galvaudé. Tel est le cas de cette délibération, dont on dira encore dans plusieurs années qu'elle a constitué un tournant.