N° 430810 – Sté Google LLC

10ème et 9ème chambres réunies

Séance du 12 juin 2020
Lecture du 19 juin 2020

CONCLUSIONS

M. Alexandre LALLET, rapporteur public

Dès l'entrée en application du RGPD, la CNIL a été saisie de deux plaintes collectives émanant d'associations et regroupant près de 10 000 personnes, dénonçant des pratiques abusives de Google lors de la configuration de terminaux mobiles fonctionnant à l'aide du système d'exploitation Android. La présidente de la Commission a diligenté en septembre 2018 un contrôle en ligne simulant le parcours d'un utilisateur qui configure un nouveau téléphone portable sous Android et qui, à cette occasion, est spontanément invité à créer un compte Google. La création d'un tel compte est tout sauf anodine, en particulier en utilisant le paramétrage par défaut. Elle permet la collecte de données à partir de l'utilisation du téléphone, de l'utilisation de différents services comme *Gmail* ou *YouTube* ou de la navigation sur des sites tiers utilisant les services de Google, notamment grâce aux cookies *Google analytics*. Ces données vont des coordonnées de la personne à l'historique de navigation et des recherches effectuées, en passant par la liste des contacts, les moyens de paiement, les contenus créés ou consultés ou encore la géolocalisation de l'équipement. Bref, la vie numérique de la personne et une partie non négligeable de sa vie réelle dont elle le reflet. Le tout appliqué à des millions de personnes.

Le contrôle de la CNIL a débouché sur une saisine de la formation restreinte, qui a estimé que Google avait manqué, d'une part, aux obligations de transparence et d'information découlant des articles 12 et 13 du RGPD et, d'autre part, aux règles relatives au recueil du consentement des personnes concernées en vue de l'utilisation de leurs données à des fins de ciblage publicitaire, fixées aux articles 4, 6 et 7 du RGPD. Elle a prononcé une amende de 50 millions d'euros, assortie d'une publication nominative de la sanction pendant deux ans, par une délibération du 21 janvier 2019 dont Google vous demande l'annulation.

La **recevabilité de l'intervention de l'association UFC - Que choisir** est longuement discutée et soulève une question assez peu explorée en jurisprudence. A notre connaissance, vous avez admis, à ce jour[1], l'intervention en défense, au soutien de l'autorité ayant prononcé

[1] A noter que, si le critère de l'intérêt suffisant utilisé de longue date en excès de pouvoir a été étendu assez

une sanction administrative, de deux types d'acteurs : d'une part, des concurrents de l'entreprise sanctionnée, à l'appui d'un pourvoi mettant en jeu le principe même d'une réglementation sectorielle[2] ; d'autre part, l'auteur de la plainte qui a débouché sur la sanction[3]. Tel n'est pas le cas en l'espèce et on peut légitimement hésiter à permettre à toute association de consommateurs d'intervenir en défense dans les recours contre toute sanction frappant une entreprise à raison de manquements à des obligations instituées au bénéfice de consommateurs, alors même qu'elle ne serait pas à l'origine de la procédure. Trois considérations nous convainquent sans hésitation de l'admettre à tout le moins ici, à l'aune de la condition libérale de « l'intérêt suffisant » : d'une part, le litige soulève des questions de principe sur l'application du RGPD à des services en ligne ; d'autre part, sont en cause des traitement massifs opérés par un acteur majeur du secteur et qui intéressent un très grand nombre de consommateurs ; enfin, et surtout, si cette association ne fait pas partie des plaignants devant la CNIL, elle porte une action de groupe contre Google devant le juge judiciaire sur les mêmes questions, et votre décision pourra peser dans l'issue de ce litige. Elle est donc, d'une certaine manière, « plaignante indirecte ».

Pour cette dernière raison, Google se plaint amèrement de la communication du dossier de procédure à cet intervenant, qui est susceptible de le réutiliser devant le juge judiciaire. Mais l'usage de ce qui n'est certes pas un droit pour l'intervenant[4] mais toujours une faculté pour le juge, est sans incidence sur le sens de la décision à rendre, donc sur celui de nos conclusions[5].

Le premier moyen soulevé pose l'une des deux questions délicates du dossier. La société se prévaut du **mécanisme de guichet unique** mis en place par l'article 56 du RGPD pour contester la compétence de la CNIL.

Le paragraphe 1 de cet article pose le principe selon lequel le contrôle des traitements transfrontaliers incombe à une **autorité chef de file**, qui est celle de **l'établissement principal** ou de l'établissement unique du responsable de traitement ou du sous-traitant. Par exception, les autres autorités nationales sont compétentes, en vertu du paragraphe 2 du même article, pour traiter les réclamations dont l'objet concerne uniquement un établissement dans

---

« récemment » en matière de plein contentieux (CE, Section, 25 juillet 2013, *OFPRA c/ E… F…*, n° 350661, au Rec.), la plupart des sanctions étaient justiciables d'un recours pour excès de pouvoir avant le « basculement ATOM » de 2009 et relevaient donc déjà du régime libéral de l'intervention en excès de pouvoir.

[2] CE, 23 février 2005, *Sté Caixa Bank France*, n° 247209, au Rec. De manière générale, le seul fait que la décision litigieuse n'ait pas d'incidence juridique directe sur l'intervenant en défense ne le prive pas de son droit à intervenir (CE, Section, 11 décembre 1998, *Association Greenpeace France et autres*, n° 194348 et a., contrairement aux conclusions de JH Stahl sur ce point : cas d'une société titulaire d'une autorisation semblable à celle qui est attaquée).

[3] CE, 12 décembre 2003, *C…*, n° 224454, au Rec.

[4] V. la décision de Section *OFPRA* mentionnée *supra*.

[5] Elle peut en revanche, dans son principe, mettre en jeu la responsabilité de l'Etat pour faute lourde (CE, Ass., 29 décembre 1978, *D…*, p 542 ; CE, 18 juin 2008, *G…*, n° 295831, au Rec.). Encore faudrait-il pouvoir démontrer que rien ne justifiait la transmission à l'intervenant – ce qui paraît difficile si l'intervention est jugée recevable - et que lui ont été communiquées des données confidentielles, dont la divulgation a porté préjudice à l'entreprise.

l'Etat membre considéré ou qui affectent sensiblement des personnes concernées dans cet Etat membre uniquement.

Il n'est ni contesté, ni contestable, que les traitements litigieux présentent un caractère transfrontalier, au sens du a) du paragraphe 23 de l'article 4 du RGPD et que la dérogation prévue au 2. de son article 56 n'est pas applicable eu égard à leur portée et à celle des plaintes dont la CNIL a été saisie. Le débat porte uniquement sur la notion **d'établissement principal** dans l'Union. Google soutient qu'il s'agit de sa filiale irlandaise. La CNIL considère que l'entreprise n'avait pas d'établissement principal dans l'Union à la date de la sanction.

Il résulte du paragraphe 16 de l'article 4 du RGPD, sous a), éclairé par le considérant 36, que l'établissement principal d'un responsable de traitement est, en principe, le lieu de son « administration centrale » dans l'Union et, par exception, un autre établissement situé dans l'Union dans lequel, le cas échéant, sont effectivement prises les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel et que cet établissement a le pouvoir de faire appliquer par les autres établissements du responsable. Le considérant 36 décline cette logique pour les groupes de sociétés, en désignant l'établissement principal du groupe d'entreprises[6].

La notion d'« administration centrale », utilisée dès la proposition de la Commission pour déterminer l'établissement principal des sous-traitants et étendue aux responsables de traitement à l'initiative du Conseil en première lecture, n'est pas définie par le RGPD. Mais il est raisonnable de penser que le législateur européen a entendu ici se référer à ce concept communément utilisé dans les textes de droit international et européen des sociétés[7], qui peut se définir comme le **centre effectif de direction et de contrôle de la société ou du groupe et de la gestion de ses intérêts**, c'est-à-dire le siège réel[8], qui peut être distinct du siège social statutaire.

---

[6] Il est précisé au considérant 37 qu'un groupe d'entreprises couvre une entreprise contrôleuse et des entreprises contrôlées, la première « *devant exercer une influence dominante sur les autres entreprises du fait, par exemple, de la détention du capital, d'une participation financière ou des règles qui la régissent, ou du pouvoir de faire appliquer les règles relatives à la protection des données à caractère personnel. Une entreprise qui contrôle le traitement de données à caractère personnel dans des entreprises qui lui sont affiliées devrait être considérée comme formant avec ces dernières un groupe d'entreprises* ».

[7] V. par exemple le règlement (CE) n° 2157/2001 du Conseil du 8 octobre 2001 relatif au statut de la société européenne. On notera que si, comme les versions françaises, les versions allemandes et espagnoles utilisent le même terme (« *Hauptverwaltung* », « *administración central* »), la version anglaise de ce règlement (et plus largement, des instruments du droit européen des sociétés : V. D. Van Gerven, *Cross-Border mergers in Europe*, Vol. 1, Cambridge university press, 2010, p. 6) utilise la notion de « *head office* » pour « *administration centrale* » alors que le GDPR évoque curieusement la « *central administration* ». V. aussi CJUE, 20 octobre 2011, *Interedil Srl*, C-396/09 pour le droit des procédures d'insolvabilité.

[8] V. le 3ème alinéa de l'article 2 de la convention de La Haye du 1er juin 1956 concernant la reconnaissance de la personnalité juridique des sociétés, associations et fondations étrangères : « *La société, l'association ou la fondation est considérée comme ayant son siège réel au lieu où est établie son administration centrale* ».

Le lieu de l'administration centrale du responsable de traitement, c'est-à-dire le siège réel de l'entreprise et, dans le cas d'un groupe d'entreprises, celui de la maison-mère, est présumé être l'établissement principal à prendre en compte pour l'application du mécanisme de guichet unique, parce qu'on suppose que c'est là que, de la même façon que les autres décisions structurantes de l'entreprise, les principales caractéristiques du traitement se décident, que la politique de protection des données personnelles traitées est conçue, pilotée et auditée et que se trouvent les interlocuteurs pertinents de l'autorité de contrôle[9] y compris, le cas échéant, le délégué à la protection des données (DPO) compétent, de sorte que les autres établissements dont l'entreprise ou le groupe dispose dans l'Union sont, à cet égard, des « exécutants »[10]. C'est la raison pour laquelle le texte permet de combattre cette présomption en démontrant qu'un autre établissement situé dans l'Union pilote en réalité le traitement. A défaut, la présomption doit jouer à plein, sans qu'il y ait à démontrer que l'administration centrale est bien en charge des questions de traitements de données. Si le législateur européen avait entendu exiger une telle démonstration, il aurait simplement écrit que l'établissement principal est le lieu où se décident les finalités et moyens du traitement.

La difficulté naît de ce que les responsables de traitement dont le siège réel est implanté en-dehors de l'Union ne peuvent bénéficier de la présomption de localisation de l'établissement principal au lieu de cette administration centrale. Il est certes tout à fait possible qu'un groupe international dispose d'un « siège régional », en Europe, qui pourra alors constituer une « administration centrale » dans l'Union au sens du RGPD. Mais il peut aussi faire le choix d'y animer un pur réseau d'établissements secondaires et de ne confier à aucun d'eux un pouvoir effectif de direction, de contrôle et de gestion sur les autres, y compris pour ce qui concerne les décisions relatives au traitement. Cette hypothèse d'absence d'administration centrale dans l'Union est expressément envisagée pour les sous-traitants par le b) du même paragraphe 16 de l'article 4 du règlement[11]. Dans ce cas, son établissement principal est le lieu où se déroule l'essentiel de ses activités de traitement dans l'Union. Le législateur européen a fait un choix différent pour le responsable de traitement, défini comme la personne qui détermine les finalités et les moyens du traitement. A défaut d'administration centrale, il y a lieu de rechercher le lieu où ces décisions sont prises ou présumées l'être, au sein de l'Union. Et si ces décisions sont prises en-dehors de l'Union, le guichet unique est fermé.

---

[9] Le paragraphe 6 de l'article 56 précise que l'autorité de contrôle chef de file est le « seul interlocuteur » du responsable de traitement pour les traitements transfrontaliers.

[10] Nous ne voyons, dans les travaux préparatoires du RGPD dont chaque partie entend se prévaloir, aucun indice déterminant en sens contraire. Le Parlement européen proposait de retenir l'établissement « *où sont prises les principales décisions quant aux finalités et aux moyens du traitement de données à caractère personnel* », faisant de la localisation du siège et de celle de l'entité la mieux placée en termes de fonctions de direction et de responsabilités administratives de simples critères d'appréciation. Sans doute pour des raisons de sécurité juridique, le Conseil a souhaité instaurer une présomption au profit du lieu de l'administration centrale. Mais nous ne pensons pas qu'il ait entendu changer radicalement de logique.

[11] « (…) *en ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant, dans la mesure où le sous-traitant est soumis à des obligations spécifiques en vertu du présent règlement* ».

Il n'y a là rien de contraire à la lettre du RGPD, qui ne garantit pas à tout responsable de traitement le droit de bénéficier de ce dispositif. Et contrairement à ce qui est soutenu, ce droit ne saurait découler du principe *non bis in idem* : si un même traitement peut faire l'objet d'une pluralité de sanctions par les autorités de contrôle européennes, celles-ci doivent apprécier la réalité et la gravité du manquement éventuel pour ce qui les concerne, c'est-à-dire dans leur champ de compétence géographique[12]. En tout état de cause, en suivant le raisonnement de la société requérante, ce principe s'opposerait seulement à ce qu'une autre autorité de contrôle que celle qui a dégainé la première prononce une sanction à raison des mêmes traitements.

Nous convenons volontiers que ce raisonnement aboutit potentiellement à priver un grand nombre de responsables de traitement extra-européens du bénéfice du guichet unique. C'est la raison pour laquelle les lignes directrices de feu le G29 du 13 décembre 2016 modifiée (WP 244 rev. 01), endossées par le comité européen de la protection des données (CEPD), suggèrent une solution accommodante pour régler ce cas de figure, consistant à regarder comme principal l'établissement désigné par le responsable de traitement et habilité par lui à faire appliquer les décisions relatives à l'activité de traitement et à assumer la responsabilité de ce traitement, notamment en disposant d'actifs suffisants. A défaut, aucune autorité chef de file ne sera désignée. Autrement dit, le responsable de traitement est invité à organiser son pilotage RGPD et en particulier, sa fonction de *compliance*, de façon à disposer d'un établissement chef de file pour prétendre au bénéfice d'une autorité chef de file.

---

[12] Ce dernier n'est pas clairement exprimé par le RGPD. Le paragraphe 1 de l'article 55 du RGPD se borne à énoncer que « *chaque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie conformément au présent règlement sur le territoire de l'Etat membre dont elle relève* », comme le faisait la directive. Sous l'empire de cette dernière, la compétence était fondée sur l'existence d'un établissement dans le cadre duquel l'entreprise procède à un traitement de données (CJUE, 1er octobre 2015, *Weltimmo*, C-230/14, pt. 35 ; CJUE, 28 juillet 2016, *Verein für Konsumenteninformation c/ Amazon EU*, C-191/15 ; CJUE, 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, C-210/16). Cette jurisprudence pourrait être transposée à l'heure du RGPD dont le champ d'application territorial est fondé sur le même critère (traitement effectué dans le cadre des activités d'un établissement). Le doute vient du 22) de l'article 4 du RGPD qui définit « l'autorité de contrôle concernée » non seulement sur la base de la présence d'un établissement sur le territoire de leur Etat membre, mais aussi, alternativement, sur le fait que des personnes résidant dans l'Etat membre sont sensiblement affectées par le traitement ou sont susceptibles de l'être, et même celles auprès desquelles une réclamation a été introduite. Cette dernière précision nous fait douter qu'on puisse tirer de cette définition un critère de compétence en qualité d'autorité de contrôle de plein exercice, car il n'est pas acceptable que les personnes concernées puissent librement choisir leur autorité de contrôle, indépendamment du lieu d'établissement du responsable de traitement ou du lieu de résidence des personnes impactées (*forum shopping*). Il nous semble donc que cette définition sert seulement à déterminer le champ des autorités de contrôle « concernées » dans le cadre du mécanisme de coopération, sous l'égide de l'autorité chef de file, et non à désigner les autorités de contrôle « compétentes » pour prononcer des sanctions. D'ailleurs, le paragraphe 3 de l'article 56 prévoit que l'autorité chef de file peut laisser le traitement d'un cas à une autorité de contrôle concernée, « *en considérant s'il existe ou non un établissement du responsable du traitement ou du sous-traitant dans l'État membre de l'autorité de contrôle qui l'a informée* », ce qui montre l'importance du critère de l'établissement, qui nous paraît au final devoir être retenu.

A notre avis, un tel assouplissement *extra-legem* ne pourrait être entériné que par la Cour de justice. Mais vous n'aurez pas besoin de la déranger pour ce motif car cette souplesse ne serait d'aucun secours pour Google.

En premier lieu, le siège social de Google LLC se trouve à Mountain View, en Californie, et rien ne permet de qualifier Google Ireland d'administration centrale de Google dans l'Union. Il vous est sommairement indiqué que cette filiale est de longue date le « siège social » du groupe en Europe. Mais d'une part, Google n'est pas enregistrée comme société européenne (SE) au sens du règlement 2157/2001 du 8 octobre 2001, lequel prévoit justement que le siège social de la SE doit être établi dans l'Etat où se situe son « administration centrale »[13]. D'autre part, l'instruction n'a pas fait ressortir que Google Ireland exercerait un quelconque pouvoir de contrôle ou de direction sur les autres filiales du groupe en Europe. Il s'agit toutes de sociétés sœurs directement détenues par la maison-mère, sans interposition capitalistique de Google Ireland, contrairement, par exemple, à ce qu'il en est d'Amazon EU au Luxembourg. Dans les limites de l'Union, Google ne constituait donc même pas un groupe d'entreprises à part entière. Et si la société requérante indique que sa filiale irlandaise avait la responsabilité de « *nombreuses fonctions organisationnelles* », nous ignorons tout de leur consistance. On peut penser qu'elle était prestataire de certains services pour ses sociétés sœurs. Mais cela ne faisait d'elle, tout au plus qu'un *primus inter pares*, la plus grosse des sœurs si vous nous permettez l'expression, mais pas la mère.

En second lieu, les finalités et les moyens des traitements relatifs à la création du compte Google lors de la configuration d'un terminal Android étaient – et sont sans doute toujours – définis dans la *Silicon Valley*, et non dans les *Docklands* de Dublin. La requête ne prétend pas le contraire. Il n'est pas plus soutenu que Google Ireland disposait de quelconques prérogatives en matière de conformité RGPD pour ces traitements déployés au sein de l'Union, notamment de services de contrôle interne et d'audit susceptibles de faire respecter la politique de groupe en matière de protection des données personnelles à l'échelle européenne. L'entreprise a du reste elle-même indiqué lors de la procédure devant la CNIL que le transfert de responsabilité de Google LLC vers la société Google Ireland Ltd pour certains traitements de données à caractère personnel concernant les ressortissants européens, conformément au mode d'emploi du CEPD, serait finalisé à la fin du mois de janvier 2019, soit postérieurement à la date de la sanction. Ainsi, même en faisant application de la soupape imaginée par le CEPD, le résultat serait le même en l'espèce.

Nous sommes d'autant moins enclin à remettre en cause la compétence de la CNIL que, dès la réception des plaintes, celle-ci a pris, sur ce point notamment, l'attache de ses homologues, qui ne l'ont pas contestée. La *Data protection commission* irlandaise a même déclaré dans la presse en 2018 ne pas être l'autorité de contrôle chef de file de Google pour ses traitements transfrontaliers, faute de pouvoirs décisionnels de Google Ireland sur les traitements. Quoique

[13] V. son article 7 : « *Le siège statutaire de la SE est situé à l'intérieur de la Communauté, dans le même Etat membre que l'administration centrale* ».

les autorités de contrôle n'ont pas la compétence de leur compétence[14], cette position unanime achève de nous convaincre d'écarter le moyen.

Vous écarterez sans hésitation les autres moyens de légalité externe.

En premier lieu, il n'y avait pas matière à saisir le CEPD, au titre du mécanisme dit de « contrôle de la cohérence », que ce soit pour avis, dans les cas énumérés à l'article 64 du RGPD, ou en vue du prononcé d'une décision contraignante au titre de sa compétence en matière de règlement des litiges, dans les hypothèses prévues à l'article 65, notamment « *lorsqu'il existe des points de vue divergents quant à l'autorité de contrôle concernée qui est compétente pour l'établissement principal* » (V. le paragraphe 1, sous b). Tel n'est pas le cas en l'espèce, comme on vient de le dire.

En deuxième lieu, le mécanisme de coopération prévu à l'article 60 du RGPD entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées est inapplicable en l'espèce, puisque, comme on vient de le voir, il n'y avait pas d'autorité chef de file dans ce dossier[15]. L'article 62 ne traite que des « opérations de conjointe » entre autorités de contrôle. Quant au dispositif d'assistance mutuelle régi par l'article 61, il est avant tout institué dans l'intérêt des autorités de contrôle et non dans celui des responsables de traitement visés par des contrôles. Il a pour but de permettre à une autorité compétente de bénéficier de l'appui de ses homologues, notamment afin d'obtenir les informations nécessaires à l'exercice de ses missions. Contrairement à ce que prétend Google, il ne prévoit nullement une forme de co-instruction des réclamations par l'ensemble des autorités européennes et encore moins de co-décision dans le prononcé de sanctions[16]. Et à supposer même qu'on exige d'une autorité compétente qu'elle tienne régulièrement informée ses homologues des contrôles qu'elle met en œuvre, dans une configuration comme la nôtre, un défaut de diligence caractériserait tout au plus un manquement, au sens du droit de l'Union, mais ne pourrait certainement pas rejaillir sur la légalité des sanctions prises par celle-ci. Le moyen est donc inopérant[17].

---

[14] Nous nous sommes tout de même demandé si cette unanimité ne condamnait pas le moyen à l'inopérance dans la mesure où le b) du paragraphe 1 de l'article 65 du RGPD prévoit qu'en cas de points de vue divergents entre les autorités de contrôle sur le lieu de l'établissement principal et, par conséquent, sur l'autorité compétente, le CEPD est saisi et désigne cette dernière par une décision contraignante. On pourrait ainsi imaginer, pour des raisons de sécurité juridique, qu'un débat sur la compétence ne puisse se tenir que si le CEPD est intervenu à la suite d'un désaccord, débat qui porterait alors, par voie d'exception, sur le bien-fondé de la position du CEPD (en cas de difficulté sérieuse, la CJUE devrait être saisie, s'agissant d'un acte d'un organe de l'Union au sens de l'article 263 du TFUE). Mais là encore, seule la Cour de justice pourrait le juger.

[15] Dans le cas où la CNIL serait autorité chef de file, il nous semble en revanche que la mise en œuvre du mécanisme, qui constitue une garantie (de cohérence), constitue une obligation dont le non-respect entacherait d'illégalité la sanction.

[16] Sous l'empire de la directive 95/46, qui instituait déjà une obligation de coopération, la CJUE a rappelé qu'une autorité de contrôle devait examiner en toute indépendance la légalité d'un traitement, ce qui incluait une complète autonomie à l'égard des autres autorités de contrôle (CJUE, 5 juin 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, C-210/16, pts. 72-73). Cette solution nous paraît valable sous l'empire du RGPD lorsque le mécanisme de l'autorité chef de file ne joue pas.

[17] Vous observerez, en tout état de cause, que la CNIL a informé les autres autorités de contrôle des plaintes dont

En troisième et dernier lieu, Google se plaint de l'empressement avec lequel la CNIL a conduit la procédure de sanction.

La société élève d'abord une **contestation de principe des règles du jeu** posées par l'article 75 du décret n° 2005-1309 du 20 octobre 2005. Le responsable de traitement mis en cause dispose d'un mois pour transmettre ses observations écrites à réception du rapport du rapporteur ; ce dernier peut, dans les 15 jours, produire des observations complémentaires au vu de la réponse apportée par le responsable de traitement, auxquelles ce dernier peut à son tour répliquer dans le même délai de quinze jours. L'instruction est alors close, sauf report décidé par la formation restreinte. L'article 76 du même décret prévoit que le responsable de traitement est informé de la date de la séance au moins un mois avant sa tenue et de la possibilité qui lui est offerte d'y être entendu, mais ce texte n'empêche pas la CNIL, comme elle l'a fait ici, d'adresser la convocation en même temps que le rapport du rapporteur, de sorte que ce préavis d'un mois ne s'ajoute pas nécessairement aux délais précédemment mentionnés. Il s'agit d'une procédure assez nerveuse, mais nous n'y décelons aucun vice structurel. Les délais minimaux sont tout à fait décents et la CNIL dispose de la souplesse pour les adapter à la complexité de l'affaire. Quant à la suppression du délai de distance d'un mois auparavant accordé par le décret de 2005 au profit des responsables de traitement établis à l'étranger, que déplore Google, elle n'est pas critiquable dans notre monde dématérialisé. C'est plutôt son maintien qui aurait été difficile à justifier.

La façon dont la CNIL a appliqué les textes en l'espèce ne donne pas plus matière à censure. Dès lors que le rapporteur a répondu aux observations de Google, sans d'ailleurs modifier ses griefs, et que la formation restreinte a accepté de repousser de 15 jours la clôture de l'instruction et la date de la séance, l'entreprise a bénéficié de **plus de trois mois**, à compter de la réception du rapport, qui contenait tous les éléments lui permettant de préparer sa défense, pour préparer ses observations orales en séance. A notre connaissance, vous n'avez jamais regardé un tel délai comme insuffisant pour l'application d'un texte ou du principe général des droits de la défense. Vous avez même admis, en l'absence même d'urgence, des délais très brefs, de l'ordre de quelques jours, notamment lorsqu'il n'était pas démontré que la personne mise en cause aurait été placée dans l'impossibilité de produire certains éléments utiles à sa défense[18] ou qu'elle avait été mise à même antérieurement de connaître le sens et les éléments d'analyse de la décision[19]. En l'occurrence, il s'agit d'une affaire sensible mais qui ne présente pas un degré de complexité, et notamment de technicité, très important ; Google ne soutient pas qu'elle aurait été privée de la possibilité de fournir des éléments supplémentaires au soutien de sa position ; enfin, elle a disposé, un mois avant le

---

elle était saisie, les a consultées pour avis et les a informées sur les investigations menées, même si ces échanges ne se sont pas poursuivis une fois la formation restreinte saisie.

[18] CE, 25 juillet 2008, *Association nouvelle des Boulogne Boys*, n° 315723, au Rec. En revanche, un délai de trois jours a été jugé insuffisant pour la suspension de la mise sur le marché d'un dispositif médical, en l'absence d'urgence (CE, 29 juillet 2002, *Sté Polytech Silimed Europe GmbH*, n° 232829, aux T.).

[19] CE, Section, 9 avril 1999, *Sté The Coca-Cola company*, n° 2014853, au Rec. : délai de 4 jours.

rapport, du procès-verbal de contrôle en ligne qui lui permettait déjà de fourbir ses armes, sans compter que les plaintes elles-mêmes ont bénéficié d'un certain écho médiatique dès leur dépôt. Quant à la barrière de la langue mise en avant par Google pour justifier les délais de traduction des quelques documents de la procédure qui n'émanent pas déjà d'elle, il n'en subsiste plus grand chose grâce, notamment, aux algorithmes développés par... Google. Nous les avons testés pour traduire quasi-instantanément la délibération attaquée, avec une remarquable fiabilité. Enfin, la CNIL a tout à fait pu faire l'économie d'une mise en demeure préalable, qui n'était pas exigée par les textes.

Au total, nous comprenons parfaitement la frustration de la société qui s'est vu opposer une fin de non-recevoir à toutes ses propositions de pourparlers alors que les enjeux auraient justifié une démarche plus interactive. Elle a ainsi pu donner à une entreprise habituée aux procédures transactionnelles et aux sanctions négociées le sentiment fâcheux de vouloir à tout prix « faire un exemple sur un GAFA », avec l'assurance d'une grande publicité. Mais cette posture est un choix institutionnel et de politique répressive qui ne saurait vicier la procédure[20].

Il est grand temps d'en venir à la **matérialité des manquements** qui sont reprochés à la société.

Nous ne pouvons faire ici l'économie d'une brève présentation du parcours utilisateur litigieux.

Lors du paramétrage du téléphone s'affiche une page intitulée « *Règles de confidentialité et conditions d'utilisation* » qui précise que « *Pour créer un compte Google, vous devez accepter les* ***Conditions d'utilisation*** *ci-dessous. De plus, lorsque vous créer un compte, nous traitons vos informations comme décrit dans nos* ***Règles de confidentialité*** (...) », ces règles étant par ailleurs accessibles par un lien hypertexte. Suivent des paragraphes d'information, notamment un paragraphe intitulé « *Pourquoi nous traitons vos données* » qui présente sommairement les différentes finalités, parmi lesquelles figure : « *proposer des annonces personnalisées, en fonction de vos paramètres de compte, via nos services, ainsi que sur les sites et les applications partenaires de Google* ». La page se termine par deux cases à cocher : « *J'accepte les conditions d'utilisation de Google* » et « *J'accepte que mes informations soient utilisées tel que décrit ci-dessus et détaillé dans les règles de confidentialité* ». L'utilisateur a ensuite le choix entre « *Ne pas créer de compte* » ou « *Créer un compte* ».

Juste avant les cases à cocher se trouve un lien déroulant intitulé « *Plus d'options* » qui permet de paramétrer le compte et d'activer certaines fonctionnalités ou de désactiver celles qui le sont par défaut, comme les annonces publicitaires personnalisées.

[20] Il faut d'ailleurs rappeler que le RGPD n'envisage pas de transaction dans ce domaine. Le droit national non plus, à supposer qu'il puisse le faire. Le paragraphe 1 de l'article 84 du RGPD laisse aux Etats membres le soin de déterminer le régime des « *autres sanctions applicables* » en cas de violation de ce règlement. On peut se demander si cette formulation les autorise à mettre en place un mécanisme de « transaction pénale ».

Si l'utilisateur n'a pas cliqué sur « *Plus d'options* » ou, l'ayant fait, s'il n'a pas modifié le paramétrage, une fenêtre pop-up s'affiche lorsqu'il clique sur « *Créer un compte* ». Cette fenêtre, intitulée « *Simple confirmation* », précise que « *Ce compte Google est configuré pour inclure des fonctionnalités de personnalisation (telles que les recommandations et les annonces personnalisées) qui sont basées sur les informations enregistrées dans votre compte. / Pour modifier vos paramètres de personnalisation et les informations enregistrées dans votre compte, sélectionnez* « Plus d'options » ». Il a alors le choix entre cliquer sur ce bouton « *Plus d'options* », ce qui le ramène à l'écran précédemment décrit, ou sur le bouton « *Confirmer* », qui permet de valider définitivement la création du compte.

Le premier grief porte sur l'obligation d'information et de transparence et, plus particulièrement, sur le défaut global d'accessibilité des informations et le manquement à l'exigence d'une information claire et compréhensible.

Il résulte des articles 12 et 13 du RGPD que le responsable de traitement est tenu de fournir, de façon **concise, transparente, compréhensible et aisément accessible**, en utilisant des termes clairs et simples, une longue série d'informations aux personnes concernées auprès desquelles il collecte des données à caractère personnel. Parmi les douze rubriques énumérées à l'article 13, on trouve les finalités du traitement et sa base juridique, la durée de conservation des données ou les critères utilisés pour la déterminer, ou encore des informations sur l'obligation ou non dans laquelle la personne se trouve de fournir les données et les conséquences éventuelles d'un refus[21].

Le RGPD pose à cet égard au responsable de traitement un défi qui n'est pas sans rappeler celui du rapporteur public : s'il n'en dit pas assez, c'est-à-dire s'il ne fournit pas les informations nécessaires à la compréhension de questions techniques ou nombreuses, il manque à son devoir de complétude de l'information ; s'il en dit trop, de peur de manquer à ce devoir, il court le risque d'endormir le lecteur - ou l'auditoire : trop d'informations tue l'information, donc l'effectivité de la garantie de transparence.

La société élève uniquement une critique en droit, centrée sur le sous-grief relatif à **l'accessibilité de l'information**, qui se compose de quatre moyens d'erreurs de droit :

- en premier lieu, elle reproche à la CNIL de ne pas avoir précisé les mesures appropriées pour satisfaire à l'exigence de transparence résultant du RGPD. Mais ce texte ne l'exige pas. La formation restreinte peut utilement faire œuvre de pédagogie, mais son rôle est d'abord de déterminer ce qu'il ne faut pas faire et qui mérite sanction ;

- en deuxième lieu, la CNIL ne s'est pas démarquée de l'approche à plusieurs niveaux recommandée par le CEPD. Dans ses lignes directrices relatives à la transparence au

[21] Contrairement au cas de la collecte de données auprès de tiers, régie par l'article 14, il n'est pas fait état expressément des catégories de données concernées parce qu'on suppose que la personne qui les fournit les connaît, mais il va de soi que l'information doit lui permettre de les identifier clairement lorsque cette fourniture n'est qu'indirecte ou différée dans le temps.

sens du RGPD[22], le CEPD recommande de ne pas faire figurer toutes les informations sur une seule page, afin de ne pas noyer d'entrée de jeu le lecteur et le dissuader de se renseigner plus avant sur la portée des traitements et leur conséquence sur leur vie privée, mais de les structurer en plusieurs niveaux, dans la limite de trois en tout – c'est-à-dire à deux clics maximum depuis la page d'entrée. Mais il résulte des termes mêmes de la délibération que la CNIL a tout à fait admis une architecture multi-niveaux. Ce qu'elle a mis en cause, c'est le nombre de niveaux et surtout la répartition des informations entre eux, aggravés par des choix contestables de présentation et de terminologie ;

- en troisième lieu, tempérant son grief précédent, la société reproche à la CNIL d'avoir à tout le moins exigé que le premier niveau d'informations soit suffisamment exhaustif pour permettre d'apprécier la portée des traitements mis en œuvre. Mais là encore, ce n'est pas le sens que nous prêtons à la délibération attaquée, qui a seulement, et à juste titre, accordé une importance particulière à ce premier niveau, y compris pour guider efficacement l'utilisateur vers les autres niveaux[23]. Elle a surtout sanctionné l'éparpillement excessif et le défaut d'accessibilité pratique des informations. Elle a par exemple relevé que cinq actions étaient nécessaires pour accéder à l'information relative à la personnalisation des annonces, six en ce qui concerne la géolocalisation et quatre pour les durées de conservation, à supposer que l'utilisateur comprenne que cette dernière catégorie d'informations se cache derrière l'intitulé « *Exporter et supprimer vos informations* » ou soit encore en état de le comprendre en parvenant à la 68ème page des Règles de confidentialité. Sur ce point, elle a même constaté, sans être contredite devant vous, que la durée de conservation de certaines données n'était tout simplement pas renseignée, sinon par la formule évasive : « *pendant de longues périodes* ».

- en quatrième et dernier lieu, la CNIL n'a pas fait application pour la première fois d'une doctrine nouvelle, en méconnaissance du principe de légalité des délits et des peines. Elle s'est bornée à appliquer le paragraphe 1 de l'article 12 du RGPD et son article 13.

Ce n'est pas la rectitude du raisonnement juridique mais le bien-fondé de **l'appréciation** portée par la CNIL qui pouvait donner davantage matière à discussion. Elle n'est pas formellement contestée par la requête, et nous pensons en tout état de cause qu'elle ne donnerait pas prise à la censure car nous sommes convaincu qu'en dépit de la complexité des

---

[22] WP26 rev. 01 du 29 novembre 2017 modifiées le 11 avril 2018.

[23] En bonne logique, ce premier niveau ne se conçoit pas comme des miscellanées portant sur certains sujets soigneusement choisis, mais comme une sorte de sommaire pédagogique, inspiré du catalogue de l'article 13 du RGPD, permettant à l'utilisateur d'accéder rapidement à la catégorie d'informations qu'il souhaite obtenir sur la base de quelques lignes synthétiques et, idéalement, illustrées. Car la meilleure façon d'être compris, c'est d'être concret et d'utiliser des exemples parlants. Un 2ème niveau consisterait à proposer une information plus développée mais didactique sur chacun des sujets, permettant de satisfaire l'utilisateur moyen ; et un éventuel troisième niveau serait une documentation technique complète ou, à tout le moins, un descriptif précis de chaque rubrique, à la manière de conditions générales de vente que seuls les consommateurs les plus désœuvrés, anxieux ou procéduriers ont l'idée d'aller lire.

traitements et de la multitude des informations à fournir, la société pouvait et devait mieux faire en termes de transparence, compte tenu des incidences sur la vie privée des utilisateurs.

*

Le second grief retenu par la CNIL touche aux conditions de **recueil du consentement en vue d'utiliser les données à des fins de personnalisation de la publicité**.

Il résulte des articles 4, 6 et 7 du RGPD que, lorsque le responsable de traitement choisit, parmi les six bases légales disponibles, de fonder son traitement sur le consentement, ce dernier doit consister en une manifestation de volonté libre, spécifique, éclairée et univoque, et se traduire par une déclaration ou un acte positif clair de la personne concernée.

La CNIL a retenu deux manquements à cet égard :

- le premier, à l'exigence d'un consentement éclairé, en raison du caractère lacunaire des informations ; sur ce point, la société se borne à renvoyer à ses développements précédents[24] ;

- l'autre, à la nécessité que ce consentement soit **spécifique et univoque** et résulte d'un acte positif clair. Ce point fait l'objet d'une contestation propre et charpentée.

Vous pourrez d'abord écarter sans difficulté deux moyens consistant à s'abriter derrière la doctrine de la CNIL en matière de cookies :

[24] La société rappelle à juste titre la doctrine du CEPD selon laquelle le consentement peut être éclairé alors même que toutes les informations prévues à l'article 13 du RGPD n'ont pas été fournies, pourvu que les « *éléments qui sont cruciaux pour faire un choix* » le soient, ce qui inclut *a minima* l'identité du responsable de traitement et la ou les finalités de ce dernier (V. le considérant 42 du RGPD). En effet, l'information exigée par les articles 12 et 13 vise non seulement à éclairer le consentement mais aussi, plus largement – notamment lorsque la base juridique du traitement n'est pas le consentement – à garantir l'effectivité des droits reconnus par le RGPD aux personnes concernées (droit d'accès, de rectification, d'opposition – effacement -, de limitation du traitement...). Il va de soi, par exemple, que l'absence de mention des coordonnées du DPO, de rappel des droits garantis par le RGPD ou de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle ne saurait vicier le consentement car ils ne sont pas nécessaires pour que la personne concernée comprenne la portée de l'engagement qu'il lui est demandé de souscrire. Le degré de précision des informations peut également être différent.
Il nous semble en outre que le **moment auquel s'apprécie la complétude de l'information** n'est pas le même selon qu'on apprécie le caractère éclairé du consentement – l'information requise doit alors être fournie avant que le consentement soit donné – ou le respect de l'obligation d'information – auquel cas, selon le 1. de l'article 13, les informations doivent être fournies « *au moment où les données en question sont obtenues* ». Ainsi, s'agissant de la création du compte Google, une grande partie des données ne sont recueillies qu'ultérieurement, lorsque le terminal et les services Google sont utilisés. Contrairement à ce qu'a estimé la CNIL à l'appui du premier grief, nous pensons donc que le message électronique postérieur à la création du compte et les outils proposés (check-up confidentialité, *dashboard*...) devaient être pris en compte. A l'inverse, ces éléments d'information postérieurs à la création du compte doivent être ignorés pour apprécier le caractère éclairé du consentement. Ce débat n'est pas élevé par Google.

- d'une part, Google se prévaut de la recommandation du 5 décembre 2013 que nous avons évoquée dans l'affaire n° 434684. La CNIL y livrait une doctrine assez accommodante du recueil du consentement pour le dépôt et la lecture de cookies. Mais cette recommandation est circonscrite à ces opérations, alors que la création du compte Google comporte aussi[25] et surtout des traitements qui sont étrangers aux traceurs de connexion. En outre, cette recommandation est dépourvue de toute portée normative et sa méconnaissance ne saurait être utilement invoquée à l'encontre d'une sanction prononcée par la formation restreinte ; enfin, cette recommandation est fondée sur la directive 95/46 alors que la sanction attaquée l'est sur le RGPD ;

- d'autre part, comme elle l'admet elle-même, Google ne peut se prévaloir de la tolérance répressive annoncée par la CNIL et dont vous avez eu à connaître[26], quant aux conséquences à tirer de la poursuite de la navigation sur le site Internet, puisque ce n'est pas ce qui est reproché à la société.

La société persiste également devant vous à entretenir l'ambiguïté sur la base juridique de son traitement, en indiquant qu'il ne repose pas seulement sur le consentement mentionné au a) du paragraphe 1 de l'article 6 du RGPD, mais aussi sur les nécessités de l'exécution d'un contrat, mentionné au b), et à ses intérêts légitimes mentionnés au f). Il n'y a pas lieu d'exclure par principe le panachage des sources de licéité du traitement[27], mais il suffit de constater que le recueil des données pour le ciblage publicitaire n'est nécessaire à l'exécution d'aucun contrat et que les intérêts économiques du responsable d'un tel traitement, aussi légitimes soient-ils, ne sauraient prévaloir sur les intérêts et les droits des personnes concernées à ne pas être « profilées » et assaillies de publicités personnalisées. Au demeurant, dès lors que la société avait fait le choix du consentement comme base légale, elle devait en respecter les exigences[28].

En outre, il ne peut être utilement reproché à la CNIL d'avoir exigé un consentement explicite qui serait réservé aux données dites sensibles par l'article 9 du RGPD. Le consentement doit également être exprès pour la généralité des données, l'article 9 posant seulement une exigence renforcée[29].

---

[25] A la lecture de la délibération attaquée, on identifie mal le raisonnement suivi par la formation restreinte pour écarter l'invocation de cette recommandation. Il semble qu'elle ait fait jouer une sorte de règle d'indépendance des législations (ePrivacy vs RGPD). Nous relevons toutefois que cette délibération évoque les données recueillies par Google grâce à ses cookies *Google analytics*, et que les règles de confidentialité Google précisent que « *Nous avons recours à plusieurs technologies pour collecter et stocker des informations, notamment les cookies, les tags de pixel, les éléments stockés en local (tels que le stockage sur les navigateurs Web ou les caches de données d'application), les bases de données et les fichiers journaux de serveur* ». En défense, la CNIL ne conteste pas qu'au nombre des traitements litigieux figurent le dépôt et la lecture de cookies.

[26] V. votre décision *Association La Quadrature du net et Association Caliopen* du 16 octobre 2019 (n° 433069, au Rec.).

[27] Les articles 13 et 14 du RGPD exigent que les personnes concernées soient informées de « *la base juridique* » du traitement. Mais il nous semble que rien n'interdit à un responsable de traitement de se fonder sur deux bases juridiques cumulativement. Une entreprise pourrait ainsi indiquer que son traitement repose sur son intérêt légitime prépondérant mais que, afin de mieux garantir les droits des personnes, elle a fait le choix de recueillir en plus leur consentement.

[28] V. en ce sens les lignes directrices du CEPD 05/2020 sur le consentement du 4 mai 2020, pts. 121-123, p. 25.

[29] La nature de ce renforcement n'est pas des plus clairs. Le CEPD y voit l'exigence d'un consentement

Le débat élevé par la société sur le caractère spécifique et univoque du consentement, et l'exigence d'un acte positif clair, est nettement plus délicat, dans son principe au moins.

La CNIL a notamment reproché à Google de ne pas proposer immédiatement à l'utilisateur la possibilité de consentir à la finalité publicitaire par une case à cocher, c'est-à-dire par un acte positif manifestant une volonté spécifique, mais de l'enfermer dans une alternative entre accepter globalement le traitement pour l'ensemble de ses finalités ou accomplir une double démarche pour ne pas consentir – en cliquant sur « *Plus d'options* » puis sur la case « *Afficher des annonces non personnalisées* », ce qui décoche *ipso facto* la case « *Afficher des annonces personnalisées* ».

Il est acquis que le consentement n'est pas valablement donné lorsque le traitement est autorisé au moyen d'une case cochée par défaut et que l'utilisateur doit décocher pour refuser de donner son consentement. C'est ce que la Cour de justice a jugé dans son arrêt Planet49 du 1er octobre dernier et dont la portée dépasse la question des cookies en litige devant elle. Mais ce précédent n'est pas directement transposable en l'espèce. Il ressort en effet des motifs de l'arrêt, éclairés par les conclusions de l'avocat général, que l'utilisateur se trouvait face à l'alternative entre, d'une part, décocher la case correspondant au consentement au traitement, de sorte que le consentement ne résultait pas d'un acte positif mais d'une simple abstention, ou, d'autre part, souscrire le service en cliquant sur le bouton général prévu à cet effet, ce qui ne pouvait être considéré comme un consentement spécifique puisque cette action emportait acceptation des autres conditions d'utilisation du service, et non simplement du traitement de données.

Comme l'indique à juste titre la requête, notre configuration est tout à fait différente. Une action positive est requise pour consentir globalement au traitement puisqu'il faut cocher la case « *J'accepte que mes informations soient utilisées tel que décrit ci-dessus et détaillé dans les règles de confidentialité* ». Le consentement est spécifique en ce sens qu'il n'est pas couplé avec l'acceptation d'autres conditions d'utilisation ou d'autres engagements, qui est l'objet de l'autre case à cocher figurant sur le même écran. Par ailleurs, une nouvelle action positive est requise lorsqu'apparaît le pop-up qui rappelle spécifiquement que le compte est paramétré de façon à inclure le ciblage publicitaire, puisque l'utilisateur doit cliquer sur le bouton « *Confirmer* » plutôt que sur « *Plus d'options* ».

Le reproche formulé par la CNIL ne se justifie pleinement que si l'on tire du RGPD l'exigence d'un consentement distinct par finalité ou, à tout le moins ici, celle d'un **consentement propre à la finalité publicitaire**. Dans ce cas, la nécessité d'ouvrir un menu dédié et de décocher une case pré-cochée contrevient bien à l'exigence que le consentement à cette finalité soit spécifique, univoque et procède d'un acte positif clair[30].

---

indubitable, résultant d'une déclaration papier signée ou d'une vérification en deux étapes (lignes directrices sur le consentement, 05/2020, v1.1., 4 mai 2020, pts. 91 et s., p. 20 et s.). Il nous semble qu'on pourrait aussi s'accommoder du recueil d'un consentement autonome, par le biais d'une case distincte du consentement au traitement de la généralité des données « non sensibles », en interprétant le terme « explicite » comme signifiant « spécifique », voire, à la limite, d'une case unique mettant clairement en exergue que sont en cause des catégories particulières de données.

Si en revanche, on estime que le RGPD n'imposait pas un consentement par finalité mais un consentement à l'échelle du traitement, rien n'interdisait à Google de recueillir un consentement global, et la possibilité que l'entreprise a offerte à l'utilisateur, sur une base qui serait alors purement volontaire, de consentir finalité par finalité, ne serait pas critiquable dès l'instant qu'elle n'a pas induit en erreur les intéressés.

Prise isolément, cette problématique nous ramène donc à la question, évoquée dans nos conclusions sur l'affaire n° 434684, de la **granularité du consentement**, qui justifierait dans son principe une question préjudicielle à la Cour de justice. Mais à la réflexion, vous pourrez, croyons-nous, vous abstenir de la lui poser, cette fois encore.

Ce que la CNIL a d'abord constaté et reproché à la société, c'est que la finalité de ciblage publicitaire n'était pas présentée de manière suffisamment claire et explicite pour que l'utilisateur puisse mesurer les conséquences de son choix. Comme nous vous l'avons dit, aucune erreur d'appréciation ne lui est reprochée, ce qui eût été vain, du reste. Les formulations très évasives utilisées dans la première page et le pop-up final sont clairement insuffisantes pour permettre à l'utilisateur de prendre la mesure de son engagement, alors que ces traitements sont particulièrement intrusifs puisque Google exploite toutes les recherches effectuées sur les services comme *Google search* ou *YouTube*, ainsi que les contenus consultés. Cette exploitation permet d'identifier les centres d'intérêts mais aussi, de proche en proche, de nombreux éléments de la vie privée ou de la personnalité de l'internaute. L'ampleur du traitement est évidemment amplifiée par la position dominante qu'occupe Google dans les moteurs de recherche et la force de ses services, comme *Gmail*, *YouTube*, *Google maps* et le *Playstore*, pour ne citer que ceux que nous utilisons le plus souvent, à titre personnel.

L'information fournie à l'utilisateur qui ne se rend pas dans le menu « *Plus d'options* » ne permettant pas, en tout état de cause, de garantir la validité du consentement, peu importe, à ce stade, qu'il soit global ou spécifique.

Il y a alors lieu d'examiner, à défaut, si un consentement valide est néanmoins recueilli en cliquant sur « *Plus d'options* ». Or d'une part, la CNIL a là encore constaté que la description de la finalité était trop floue. L'appréciation est plus sévère car il est notamment fait référence aux recherches *Google* et *YouTube*, mais ce point n'est pas critiqué par la requête et il est vrai que la formulation retenue par la société impose de lire entre les lignes ou de combiner plusieurs ressources documentaires éparpillées, alors qu'elle aurait pu, sans excès littéraire ni innovation ergonomique, être plus explicite sur cet écran. D'autre part, pris de manière autonome, ce menu ne respecte pas l'exigence d'un acte positif clair manifestant le consentement de manière univoque puisque la case est déjà cochée, contrairement d'ailleurs à d'autres rubriques.

---

[30] Vous noterez au passage que, contrairement à ce qui est soutenu, cette position n'interdit pas par ailleurs au responsable de traitement d'offrir la possibilité de consentir en un clic à l'ensemble des finalités affichées, par un bouton « *Accepter tout* », pour des raisons d'ergonomie, pourvu qu'il ait aussi la possibilité de « faire son marché » parmi les finalités présentées.

Dans ces conditions, il importe peu que la CNIL ait cru devoir ajouter que le consentement aurait dû, dès le premier niveau, être recueilli de manière distincte pour la finalité de ciblage publicitaire. Ce motif est surabondant ou, si vous préférez vous placer dans l'épure de la jurisprudence *Ministre de l'économie et des finances c/ Dame P…* du 12 janvier 1968 (Rec. p. 39)[31], nous sommes certain que la CNIL aurait pris la même décision, dans son principe comme dans son montant, indépendamment de la question de la granularité du consentement[32]. C'est ce qu'elle vous indique dans sa dernière production. Dans un tel cas, une question préjudicielle serait superflue et, le cas échéant, irrecevable.

Les derniers moyens critiquant le **quantum de la sanction** pourront être aisément écartés.

En premier lieu, si la CNIL était tenue de prendre en compte l'ensemble des critères d'appréciation énumérés au paragraphe 2 de l'article 83 du RGPD, et si l'article L. 211-5 du code des relations entre le public et l'administration l'obligeait à faire état des considérations de droit et de fait fondant sa décision, aucun texte, notamment le RGPD, ni aucun principe ne lui faisait obligation de motiver sa décision au regard de chacun de ces critères, contrairement à ce qui est soutenu (V. sur ce dernier point : CE, 19 octobre 2016, *Ministre de l'agriculture, de l'agroalimentaire et de la forêt c/ EARL Sapins du Bocage*, n° 386405, aux T.)[33]. Il n'y a donc pas d'insuffisance de motivation. Par ailleurs, rien ne donne à penser que la CNIL aurait ignoré des critères d'appréciation pertinents. Sa délibération indique elle-même l'inverse. Elle n'est donc pas entachée d'erreur de droit.

En second lieu, l'amende prononcée ne saurait être regardée comme disproportionnée.

---

[31] La jurisprudence *Dame P…* a été maintes fois appliquée en matière de sanctions disciplinaires (V. par exemple : CE, 21 février 1969, *Ministre c/ K…*, Rec. p. 112 ; CE, 27 novembre 1996, *Epoux W… et époux C…*, n° 170209, au Rec. ; CE, 29 décembre 2000, T…, n° 197739-202564-202565, au Rec. ; et en matière de référé : JRCE, 12 mai 2005, *Z…*, n° 279011, aux T.). C'est d'ailleurs cette matière qui a été le terrain d'expérimentation d'une jurisprudence à l'époque audacieuse et qui a inspiré la jurisprudence *Dame P…*, consistant à rechercher si le motif légal aurait à lui seul entraîné la décision prise (CE, 14 janvier 1948, *C…*, au Rec. p. 18). Il n'y a aucune raison de ne pas en faire application dans l'ensemble de la matière répressive, dans laquelle vous avez d'ailleurs admis la substitution de motifs relatifs à un « même manquement » (CE, Section, 23 novembre 2001, *Compagnie nationale Air France*, n° 195550, au Rec.). A cet égard, nous relevons que vous ne vous êtes pas livré dans ce dernier cas à l'examen contrefactuel que vous menez en excès de pouvoir depuis la décision *H… (n° 240560)* (postérieure) et qu'on retrouve dans la jurisprudence *Dame P…*, consistant à déterminer, au vu de l'instruction, si l'autorité aurait effectivement pris la même décision. Il nous semble toutefois que cet examen est nécessaire, aussi bien sur le principe de la sanction que, surtout, sur son quantum, en matière de neutralisation des motifs illégaux, que le juge peut effectuer d'office.

[32] Alternativement, ce motif précis, qui s'analyse en quelque sorte comme un sous-grief, pourrait être regardé comme illégal, faute pour la CNIL d'avoir recherché si l'absence de recueil spécifique du consentement par un acte positif clair pour la finalité de ciblage publicitaire méconnaissait le caractère libre du consentement, qui nous paraît être le fondement adéquat. Sur le fond, nous relevons que, parmi les finalités présentées figurent « *Améliorer la qualité de nos services et en développer de nouveaux* » et, surtout « *Renforcer la sécurité en vous protégeant contre la fraude et les abus* ». L'utilisateur aura donc tendance à accepter l'ensemble des finalités pour ne pas se priver de cette protection. Et s'il peut renoncer purement et simplement à créer un compte Google, cette création est présentée comme une condition pour que son appareil « fonctionne mieux » et pour pouvoir effectuer certaines actions, notamment l'activation des fonctionnalités de protection du téléphone. Il n'est donc pas évident d'y voir un consentement libre.

[33] V. aussi CE, Section, 27 mai 2002, *Société Guimatho*, n° 229187, au Rec.

Le maximum encouru par Google, eu égard aux manquements commis, s'élevait à 4 % de son chiffre d'affaires mondial, soit 3,8 Md€. **La sanction prononcée représente environ 0,05 % de ce chiffre d'affaires et 1,3 % de l'amende plafond**.

Par leur **nature**, ces manquements présentent une réelle gravité puisqu'ils touchent à la question sensible du consentement et à l'obligation d'information et de transparence qui conditionne l'effectivité des droits garantis par le RGPD. La gravité de leurs **effets** est, quant à elle, tout à fait considérable compte tenu à la fois du nombre d'utilisateurs concernés, dont les 10 000 plaignants représentés ne sont qu'un petit échantillon, de l'ampleur des opérations mises en œuvre et du nombre, de la variété et de la sensibilité des données exploitées, surtout par croisement, recoupement et analyses algorithmiques de toutes natures. Un tel traitement est certainement au nombre de ceux qui requièrent une analyse d'impact sur la vie privée en raison de leur sensibilité et de leur échelle. La CNIL a également tenu compte à juste titre de l'avantage que la société a pu retirer de ces manquements, eu égard à la place du ciblage publicitaire dans son modèle économique.

Elle a enfin relevé que le manquement perdurait à la date de sa sanction, mettant ainsi en exergue son caractère continu et sa durée. Implicitement, elle y a vu des manquements délibérés, par opposition à de simples négligences, même si nous convenons volontiers que les violations du RGPD reprochées prêtent à discussion et ne sont pas l'œuvre d'un responsable de traitement voyou, comme il en existe.

Le choix de recourir à une sanction pécuniaire est donc justifié, et l'amende prononcée, assortie d'une publication nominative pendant deux ans, est raisonnable, quand bien même d'autres autorités de contrôle auraient, semble-t-il, la main moins lourde pour des manquements prétendument comparables.

Dans ces conditions, nous vous invitons, après avoir admis l'intervention, à rejeter la requête. Tel est le sens de nos conclusions.