N° 434684 – Association des agences conseil en communication et autres

10ème et 9ème chambres réunies

Séance du 12 juin 2020
Lecture du 19 juin 2020

CONCLUSIONS

M. Alexandre LALLET, rapporteur public

Au risque de sentir le réchauffé, les cookies sont de retour dans votre prétoire. Souvenez-vous l'été dernier, la CNIL a entrepris de faire évoluer sa doctrine à l'égard des traceurs de connexion que les éditeurs de site ou les tiers agissant pour leur compte déposent sur vos appareils et exploitent aux fins les plus diverses. Elle a remplacé sa recommandation de 2013 par une délibération n° 2019-093 du 4 juillet 2019, en marge de laquelle elle a annoncé, par un communiqué de presse que vous avez refusé d'annuler[1], qu'elle ne sanctionnerait pas les opérateurs qui continueraient de présumer que l'internaute qui poursuit sa navigation sur un site consent au dépôt et à l'utilisation des cookies, le temps d'édicter de manière concertée une recommandation sur les modalités techniques du recueil du consentement.

Plusieurs associations professionnelles appartenant ou gravitant autour du secteur du marketing digital vous saisissent d'une demande d'annulation de la délibération elle-même.

Selon les termes de son préambule, la CNIL a entendu adopter des « *lignes directrices* »[2] ayant pour objet de « *rappeler le droit applicable aux opérations de lecture ou écriture dans le terminal d'un utilisateur, et notamment l'usage des cookies et autres traceurs* ». Elle y présente sa doctrine d'interprétation de la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dite « *directive ePrivacy* », transposée par l'article 82 de la loi du 6 janvier 1978, ainsi que du RGPD, en particulier de ses dispositions relatives au consentement. Et elle annonce que la méconnaissance de ces règles sera passible de sanctions.

---

[1] CE, 16 octobre 2019, *Association La Quadrature du Net et Association Caliopen*, n° 433069, au Rec.

[2] Naturellement, vous n'êtes pas lié par cette qualification, directement empruntée à l'article 70 du RGPD qui assigne au comité européen de la protection des données (CEPD) la mission de publier des « *lignes directrices, des recommandations et des bonnes pratiques* » sur plusieurs volets de cette réglementation. Ce vocable a été servilement repris par le b) du 2° de l'article 8 de la loi du 6 janvier 1978, qui confie à la CNIL le soin d'établir et publier « *des lignes directrices, recommandations ou référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel* ». Nous n'avons pas identifié de travaux de référence éclairant ces différences terminologiques. Il nous semble que les « lignes directrices » se veulent plus prescriptives que des « recommandations » et « référentiels », tandis que les « bonnes pratiques » se réfèrent à des pratiques exemplaires constatées chez certains responsables de traitement et que l'autorité de contrôle entend promouvoir.

Cette délibération, que la CNIL présente sur son site Internet comme une « *synthèse du droit applicable* », annonce par ailleurs qu'elle sera complétée par des recommandations sectorielles, qui, elles, ont seulement pour objet de guider les professionnels concernés dans leur démarche de mise en conformité, en décrivant des « *modalités pratiques possibles* » de recueil du consentement et des bonnes pratiques. La CNIL précise en outre qu'en cas de manquement aux dispositions applicables, elle pourra prendre « *toutes mesures correctrices et sanctions vis-à-vis des organismes qui y sont soumis* ».

Il est tout à fait certain que cette délibération a pour objet d'influer de manière significative sur les comportements des opérateurs dans le recours aux cookies et est de nature à produire des effets notables sur les pratiques et sur l'économie du secteur du marketing digital dont les requérants sont des représentants. A nos yeux, l'essentiel de la délibération relève même plus radicalement de la première branche issue de la décision d'Assemblée *Fairvesta*[3], celle qui traite des avis, recommandations ou prises de position qui revêtent le caractère de dispositions générales et impératives. L'acte dont vous êtes saisi se présente à titre principal comme une communication interprétative, pour reprendre le vocable de la Commission européenne, comme la « position » par laquelle l'Autorité de contrôle prudentiel et de résolution a exposé, de façon générale et impérative, son interprétation d'une notion figurant dans le code monétaire et financier (CE, 30 juin 2016, *Crédit agricole SA et autres*, n° 383822, aux T.)[4].

Naturellement, il est fréquent que les actes de droit souple présentent un caractère composite, comme le relevait l'Assemblée générale dans sa célèbre étude en plaidant, sans grand succès, pour une dissociation formelle plus claire entre les parties impératives et les simples recommandations[5]. S'il s'avère, au vu de la rédaction employée sur tel ou tel point ou de l'économie générale d'un passage, que la CNIL a entendu se séparer de la logique énoncée en préambule et se limiter à une recommandation de bonne pratique, il y a lieu d'en prendre acte et d'adapter votre contrôle en conséquence[6], donc de ne l'annuler que si elle invite ses destinataires à se livrer à des agissements prohibés. Nous y reviendrons au cas par cas.

---

[3] CE, 21 mars 2016, *Société Fairvesta International GMBH et autres*, n°s 368082 368083 368084, au Rec.

[4] La rédaction de sa délibération est nettement plus prescriptive que celle de la délibération n° 2013-378 du 5 décembre 2013 qu'elle abroge, qui se bornait à adopter une « recommandation » présentant, plus prudemment, « *les principes qu'il conviendrait de respecter* », et qui ne faisait à aucun moment état des pouvoirs répressifs de la Commission.

[5] Elle préconisait dans sa proposition n° 13, de « *les distinguer clairement par des règles de présentation ne laissant pas de place à l'ambiguïté* ». La CNIL ne l'a pas fait, mais cela ne doit pas vous empêcher de vous livrer à ce travail d'échenillage, qui vous est familier au moins depuis la jurisprudence de Section *D...* (n° 233618), consistant à examiner la formulation de chacune des dispositions attaquées pour déterminer sa portée exacte. Il pourra ainsi s'agir, selon les alinéas, de l'interprétation d'une disposition législative ou réglementaire « imposée » aux responsables de traitement, d'une simple recommandation de bonne pratique et, entre les deux, d'authentiques lignes directrices guidant le pouvoir répressif de l'autorité et dont elle pourrait s'écarter au cas par cas, en considération de la situation particulière qui lui est soumise ou de motifs d'intérêt général. Nous notons que vous avez aussi été amené à distinguer les parties de lignes directrices dont l'illégalité pouvait être utilement invoquée par voie d'exception et les autres, en particulier celles qui se bornent à décrire le contexte dans lequel s'inscrivent les appréciations de l'autorité (CE, 13 décembre 2017, *Sté Bouygues Télécom et autres*, n° 401799-401830-401912, au Rec.).

[6] Dans la seconde branche de la décision *Fairvesta*, le juge doit, dans l'examen des vices susceptibles d'affecter leur légalité, tenir compte de leur nature et de leurs caractéristiques, ainsi que du pouvoir d'appréciation dont dispose l'autorité de régulation. Cette modulation de l'office du juge n'a guère été éclairée par la jurisprudence

Ces précisions étant apportées, nous pouvons à présent déclarer ouverte la séance de ball-trap contentieux, qui se compose d'une dizaine de moyens assortis de treize propositions de questions préjudicielles.

*

Pour s'échauffer, rien de tel qu'un tir à blanc : il est reproché à la CNIL, sans plus de précision, de ne pas avoir respecté les **règles de procédure** qui s'imposent à elle. Or le dossier ne fait ressortir aucune irrégularité, notamment quant à la convocation des membres, aux règles de quorum et de majorité, et à la présence du commissaire du Gouvernement.

*

La deuxième salve est plus sérieuse. Elle est tirée de **l'incompétence de la CNIL** à avoir traité de cookies et traceurs ne portant pas sur des données à caractère personnel.

Le champ d'application de la directive ePrivacy est plus large que celui de la réglementation en matière de protection des données à caractère personnel. Le paragraphe 3 de son article 5, issu de la directive 2009/136/CE du 25 novembre 2009, qui encadre les opérations de dépôt et de lecture des traceurs de connexion, se borne à évoquer le stockage et l'accès à des « *informations* », qui peuvent présenter ou non un caractère personnel. Toutefois, le législateur européen a veillé à articuler les deux corps de règles. Lorsqu'en 2009, il a introduit l'exigence d'un consentement préalable au dépôt et à la lecture de cookies, c'est-à-dire un régime d'*opt-in*, en lieu et place du régime d'opposition, c'est-à-dire d'*opt-out*, institué en 2002, il a renvoyé, pour la définition du consentement, à la directive 95/46/CE et, désormais, au RGPD, puisque l'article 94 de ce règlement remplace la référence à cette directive par une référence au RGPD dans tous les textes en vigueur, y compris la directive ePrivacy. Ce renvoi est assez logique car, en pratique, la très grande majorité des cookies impliquent des données à caractère personnel. Il en résulte, comme l'a jugé clairement la Cour de justice de l'Union européenne, que les dispositions de la directive ePrivacy « *ne doivent pas être interprétés différemment selon que les informations stockées ou consultées dans l'équipement terminal de l'utilisateur d'un site Internet constituent ou non des données à caractère personnel au sens de la directive 95/46 et du règlement 2016/679* » (CJUE, Grande chambre, 1er octobre 2019, *Bundesverband des Verbraucherzentralen und Verbraucherverbände c/ Planet49 GmbH*, C-673/17)[7].

---

postérieure. Il y a lieu d'observer que la décision du 13 décembre 2017, *Société Bouygues Télécom et autres* (n° 401799-401830-401912, au Rec.), qui transpose la jurisprudence *Fairvesta* aux lignes directrices, laisse entendre, par sa construction, que l'office adapté serait circonscrit à la seconde sous-branche de la seconde branche de Fairvesta (actes ayant pour objet d'influer de manière significative sur les comportements). Mais nous pensons qu'il s'agit d'un copier-coller partiel et malencontreux du considérant de principe de la décision *Fairvesta*, qui élude la première branche.

[7] Telle était de longue date la doctrine du G29 (cf. avis relatif à la publicité comportementale en ligne du 22 juin 2009).

Le législateur français a logiquement fait le choix de transposer la directive ePrivacy dans la loi n° 78-17 du 6 janvier 1978, d'abord au II de l'article 32 – article alors consacré au droit d'information des personnes concernées à l'égard des traitements de données à caractère personnel - puis à l'article 82, sans en circonscrire le champ d'application aux données à caractère personnel. Il y a simplement introduit la notion de « responsable de traitement » qui est un vocable propre au droit de la protection des données à caractère personnel ignoré de la directive ePrivacy, laquelle se borne à évoquer des « traitements ». Cela étant, sauf à placer la France en situation de manquement, il n'est évidemment pas possible de restreindre le champ d'application de l'article 82 aux seules données à caractère personnel, puisqu'il n'existe aucun autre texte national traitant de ce sujet pour le surplus.

La petite difficulté tient à ce que le champ de compétence de la CNIL, lui, n'a pas été expressément adapté en conséquence. A la lettre, l'article 8 de la loi de 1978 l'investit seulement de la mission de veiller à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de cette loi et il n'envisage pas l'élaboration de lignes directrices et de recommandations au-delà de ce champ. Mais il n'y a là, à nos yeux, qu'un expédient rédactionnel. Nous sommes absolument persuadé qu'en insérant les dispositions relatives aux cookies dans la loi du 6 janvier 1978, le législateur a entendu reconnaître à cette autorité une compétence pleine et entière dans ce domaine.

Nous relevons à cet égard que les articles 16 et 20 de la loi du 6 janvier 1978 permettent le prononcé par la CNIL de mesures correctrices et de sanctions en cas de manquement « aux dispositions de cette loi » sans limiter formellement sa compétence aux traitements de données à caractère personnel. A la lettre, elle peut donc sanctionner toute méconnaissance de l'article 82 de cette loi, quelle que soit la nature des informations en cause. Elle a donc nécessairement compétence pour édicter une doctrine interprétative de ces dispositions.

Il serait du reste parfaitement artificiel, voire absurde, d'ériger une frontière étanche entre les deux catégories de cookies, qui peuvent être utilisées par les mêmes éditeurs à l'occasion des mêmes opérations de dépôt et d'exploitation. C'est la raison pour laquelle, dès 2013, la recommandation de la CNIL abordait aussi les traceurs n'impliquant pas de données personnelles, sans que cette initiative n'émeuve personne à l'époque. Et il serait tout à fait fâcheux, voire contraire au droit de l'Union[8], de laisser une partie de ce régime sans autorité de contrôle dédiée.

---

[8] L'article 15 bis de la directive ePrivacy exige des Etats membres qu'ils désignent une ou plusieurs autorités nationales compétentes, chargée(s) notamment d'en contrôler le respect et de sanctionner les contrevenants. Si certains pays ont désigné à la fois leur autorité compétente en matière de protection des données personnelles et leur autorité de régulation du secteur des télécoms (V. sur ce point le « *report to the Commission "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation »*, SMART 2013/0071, pp. 33 (pt. 3.2.3), tel n'est pas le choix de la France : dans son tableau de suivi des autorités de contrôle de la directive ePrivacy figurant sur son site Internet, la Commission européenne mentionne uniquement la CNIL, pour ce qui concerne la France. Selon ce tableau, outre la France, l'Italie, le Royaume-Uni, l'Irlande, l'Espagne, le Portugal, la Pologne, la République Tchèque, la Roumanie, Bulgarie, l'Estonie, la Lituanie, la Lettonie, le Luxembourg et Malte ont confié la supervision de la directive e-privacy exclusivement à « leur CNIL », les autres pays ayant prévu une compétence partagée avec « leur ARCEP ». Les articles L. 36-5 et suivants du code des postes et des communications électroniques ne font à aucun moment figurer la mise en œuvre de la directive ePrivacy et de ses dispositions nationales de transposition dans les

Ajoutons pour terminer sur ce point qu'il n'est pas dans vos habitudes de définir de manière restrictive le champ de compétence des autorités de régulation. Vous veillez, sans vous sentir ligoté par la lettre des textes, à leur reconnaître le pouvoir réglementaire nécessaire à l'accomplissement de leur mission générale (CE, 10 juillet 2013, *SAS AT&T Global Network Services France*, n° 360397, au Rec.) et, *a fortiori*, à leur permettre de prendre des actes de droit souple à cette fin (décision *Fairvesta*).

*

Dans la foulée du moyen précédent, vous pourrez écarter le moyen d'erreur de droit consistant à reprocher à la CNIL d'avoir appliqué aux traceurs de connexion ne portant pas sur des données à caractère personnel, les exigences du RGPD en matière de consentement au traitement de données à caractère personnel. C'est ce qu'a jugé la Cour de justice, comme nous l'avons vu.

*

Il est ensuite reproché à la CNIL d'avoir commis une **erreur de droit en conférant une force obligatoire aux lignes directrices du CEPD**, au lieu d'exercer elle-même la compétence que lui confie la loi de 1978. Mais rien ne permet de penser qu'elle se serait estimée juridiquement liée par ces productions du CEPD – ce qu'elle nie devant vous - ni qu'elle y aurait vu des actes directement applicables en droit français, ce qu'elles ne sont pas juridiquement[9]. Elle s'est bornée à en rappeler la teneur voire à y adosser sa propre doctrine, comme nous allons le voir maintenant.

*

Nous en venons au cœur de la contestation élevée devant vous, qui porte sur la possibilité pour les opérateurs de subordonner l'accès à leur site ou à certains de ses contenus à l'acceptation des cookies – ce qu'on appelle usuellement dans le jargon, les « ***cookie walls*** » ou l'approche « *à prendre ou à laisser* ». L'objectif est bien connu : plutôt que de faire payer l'accès au service en monnaie sonnante et trébuchante, les éditeurs des sites qui recourent à

---

missions de l'ARCEP, laquelle n'a pas soufflé mot, dans son avis du 10 mai 2011 sur le projet d'ordonnance relative aux communications électroniques qui a ajouté l'exigence du consentement par transposition de la directive de 2009, de ces dernières dispositions, alors que la CNIL, dans son avis n° 2011-161 du 9 juin 2011, les commente abondamment et relève même qu'elles s'appliquent y compris en l'absence de données personnelles. Elle est d'ailleurs compétente, en vertu de l'article L. 34-5 du même code, pour connaître de l'encadrement de la prospection directe par voie électronique issue de la directive ePrivacy (mais il est vrai que cette démarche implique nécessairement un traitement de données à caractère personnel). Par ailleurs, aucune sanction pénale n'a été instituée lorsque les données collectées ne présentent pas un caractère personnel. S'agissant en revanche des données à caractère personnel, l'article 226-18 du code pénal prohibe leur collecte déloyale ou illicite. Il n'est pas exclu par ailleurs que la DGCCRF puisse intervenir là où la CNIL ne le pourrait pas si sa compétence était limitée aux données personnelles, mais nous ne sommes pas du tout persuadé que la Commission européenne se contenterait de cette compétence implicite et hypothétique.

[9] A la différence des décisions contraignantes que ce comité peut être amené à prendre dans les hypothèses limitativement énumérées à l'article 65 du RGPD.

cette pratique valorisent les données personnelles des internautes auprès des autres acteurs du marketing digital à des fins de ciblage publicitaire notamment. C'est donc l'équilibre économique d'un secteur, tel qu'il est aujourd'hui conçu, qui est en jeu.

La directive ePrivacy de 2002 ne comportait aucune prohibition de principe des cookie walls. Au contraire, son considérant 25 précisait que « *l'accès au contenu d'un site spécifique peut être, toutefois, subordonné au fait d'accepter, en pleine connaissance de cause, l'installation d'un témoin de connexion ou d'un dispositif analogue, si celui-ci est utilisé à des fins légitimes* », par opposition à l'utilisation détournée ou frauduleuse. C'est sur la base de ce considérant que, lors des débats qui ont accouché de la loi n° 2004-801 du 6 août 2004 qui a transposé cette directive, l'idée d'une interdiction des *cookie walls* a été expressément écartée par le législateur national[10].

Comme on l'a dit, la directive ePrivacy a été modifiée en 2009 pour instaurer le régime du consentement préalable. Le f) de son article 2 précise que la notion de consentement au sens de cette directive correspond au « *consentement de la personne concernée figurant dans la directive 95/46/CE* »[11], c'est-à-dire « *toute manifestation de volonté, libre[12], spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». Vous noterez toutefois qu'aucun considérant[13] ni aucune disposition de la directive de 2009 n'est revenu sur le considérant 25 de la directive d'origine. Et ni le rapport au Président de la République sur l'ordonnance de transposition[14], ni les travaux préparatoires de la loi de ratification[15], n'offre d'indices d'une volonté de revenir sur la possibilité de conditionner l'accès à un site à l'accord sur le dépôt et la lecture des cookies, expressément admise en 2004.

Le débat sur la licéité de cette pratique a surtout été relancé par l'entrée en application du RGPD et le durcissement des exigences en matière de recueil du consentement, notamment, pour ce qui nous intéresse ici, en matière de **liberté du consentement**.

C'est à ce titre que la CNIL aborde la question à l'article 2 des lignes directrices attaquées :

---

[10] Alors que l'Assemblée nationale avait, en première lecture et avant l'adoption de la directive ePrivacy, interdit cette pratique, avec un avis de sagesse du garde des sceaux plaidant pour approfondir la question dans le cadre de la navette parlementaire, le Sénat est revenu sur cette interdiction en se référant au considérant 25 de la directive et en plaidant pour une mise en conformité stricte avec celle-ci (V. Rapport n° 218 (2002-2003) de M. Alex TÜRK, fait au nom de la commission des lois, déposé le 19 mars 2003, pp. 116-117).

[11] Si le paragraphe 3 de l'article 5 de la directive ePrivacy évoque non le consentement, mais « l'accord » de l'internaute, il s'agit à l'évidence d'un glissement rédactionnel fortuit, sinon d'une erreur de traduction, qu'on ne retrouve pas dans la version anglaise et que la Cour de justice a neutralisée dans l'arrêt que nous avons mentionné. V. aussi en ce sens l'avis rendu par la CNIL sur le projet d'ordonnance relative aux communications électroniques de 2011 qui a transposé la directive de 2009.

[12] C'est nous qui soulignons.

[13] Le considérant 66 de la directive de 2009, qui explicite le passage à l'*opt-in*, est même d'une grande prudence rédactionnelle.

[14] Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques.

[15] Loi n° 2014-1 du 2 janvier 2014 habilitant le Gouvernement à simplifier et sécuriser la vie des entreprises (art. 18)

- elle commence, au 4ème alinéa, par poser sa propre doctrine : « *La Commission considère que le consentement ne peut être valable que si la personne concernée est en mesure d'exercer valablement son choix et ne subit pas d'inconvénients majeurs en cas d'absence ou de retrait du consentement* ».
- Puis au 5ème alinéa, elle illustre cette doctrine en se prévalant de la position adoptée en dernier lieu par le CEPD : « *A ce titre*[16]*, la Commission rappelle que le CEPD, dans sa « déclaration sur la révision de la directive « ePrivacy » et son incidence sur la protection de la vie privée et la confidentialité des communications électroniques », a considéré que la pratique qui consiste à bloquer l'accès à un site web ou à une application mobile pour qui ne consent pas à être suivi (« cookie walls ») n'est pas conforme au RGPD. Le CEPD considère en effet que, dans une telle hypothèse, les utilisateurs ne sont pas en mesure de refuser le recours à des traceurs sans subir des conséquences négatives (en l'occurrence l'impossibilité d'accéder au site consulté)* ».

Le rappel de la position du CEPD qui figure au 5ème alinéa est, par lui-même, à l'abri de la critique. Non pas parce qu'un tel rappel serait soustrait à tout contrôle. S'il ne vous appartient pas de porter une appréciation sur la rectitude de la position du CEPD, organe de l'Union[17], nous pensons que vous devez, saisi d'un moyen en ce sens, vous assurer que l'interprétation qui en est donnée par une autorité de régulation dans une recommandation ou une position n'en méconnaît pas le sens et la portée, comme vous l'avez fait d'une circulaire interprétant une décision de la Cour de cassation (CE, 23 juillet 2017, *Association enfances et famille d'adoption*, n° 347677, aux T.). Il y a là un enjeu majeur de sécurité juridique alors qu'une interprétation biaisée d'un tel document peut entraîner des effets tout à fait massifs et nocifs. Mais en l'occurrence, la CNIL a correctement interprété la déclaration du CEPD. Ce dernier a émis le souhait que le règlement qui a vocation à se substituer à la directive ePrivacy explicite ce qui, à ses yeux, est déjà l'état du droit, à savoir que les *cookie walls* sont incompatibles avec le RGPD. Le CEPD a d'ailleurs entériné cette doctrine, sans nuances, dans la dernière mouture de ses lignes directrices sur le consentement, parues le 4 mai dernier[18].

Nettement plus délicate est la critique qui vise la doctrine de la CNIL elle-même. Précisons d'abord qu'au vu de la rédaction de la délibération, vous n'êtes pas face à une simple recommandation de bonne pratique, mais à une doctrine interprétative susceptible de fonder des sanctions. Et sa portée ne fait aucun doute, notamment du fait de la locution « à ce titre » : il s'est bien agi de proscrire les *cookie walls*. La CNIL confirme du reste dans son mémoire en défense qu'à ses yeux, un internaute qui se voit refuser l'accès à un site Internet à défaut d'accepter le suivi de sa navigation ne se voit pas offrir un choix réel, de sorte que son consentement n'est pas valable. Vous noterez qu'elle ne fait, ce faisant, que reprendre en substance ce qui figurait déjà, quoique de manière moins comminatoire, dans sa recommandation de 2013, dans laquelle elle évoquait des « *conséquences négatives importantes* » s'attachant au refus de consentement, au nombre desquelles elle rangeait l'impossibilité d'accéder à un site Internet.

[16] C'est nous qui soulignons.
[17] V. le paragraphe 1 de l'article 68 du RGPD.
[18] Lignes directrices 05/2020 sur le consentement au sens du RGPD, version 1.1, 4 mai 2020, pt. 39

Le problème vient de ce qu'une telle prohibition n'est posée par aucune disposition du RGPD, qui reprend le principe de liberté du consentement figurant déjà dans la directive 95/46. Le paragraphe 4 de l'article 7 du RGPD se borne à guider l'appréciation du caractère libre ou contraint du consentement, en prévoyant que, dans cet exercice, « *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* ». Autrement dit, une vigilance particulière s'impose lorsqu'un responsable de traitement utilise le levier que lui offre un contrat ou un service en ligne pour recueillir le consentement d'une personne à la réalisation d'un traitement qui n'est pas nécessaire à son exécution, c'est-à-dire se livre à une pratique de couplage (*bundling*)[19]. Mais si le législateur européen avait entendu prohiber cette pratique par elle-même, il n'aurait pas rédigé le règlement de cette manière. Il y a lieu d'observer au surplus que, parmi les cas de licéité des traitements énumérés à l'article 6, figure déjà, aux côtés du consentement, la rubrique des « *traitements nécessaires à l'exécution d'un contrat auquel la personne concernée est partie* »[20]. Le paragraphe 4 de l'article 7 ne peut donc avoir pour objet de circonscrire le consentement à des traitements nécessaires à l'exécution d'un contrat et qui sont donc dispensés de l'obligation de recueil du consentement[21].

Sans doute le considérant 43 du RGPD pose-t-il une véritable **présomption** d'absence de liberté du consentement en cas de couplage. Mais outre que celle-ci ne trouve aucun appui dans le corps du RGPD, il s'agit simplement d'une présomption dont, jusqu'à récemment encore, le G29 puis le CEPD admettaient qu'elle puisse être renversée, fût-ce de manière très exceptionnelle[22]. On trouve ainsi sous sa plume l'idée que les cookie walls étaient « *rarement légitimes* »[23]. Le contrôleur européen de la protection des données était du même avis en 2017, en recommandant une approche casuistique[24]. C'est seulement dans son dernier avis sur le projet de règlement ePrivacy et, surtout, pour faire bonne mesure, dans la dernière version de ses lignes directrices sur le consentement de mai dernier que le CEPD a entendu proscrire de manière générale et absolue les *cookie walls*, alors même que les textes n'ont pas changé.

Le soubassement doctrinal de cette position est que les données à caractère personnel devraient être des biens hors commerce que les personnes concernées ne pourraient monnayer, consciemment ou non, en contrepartie d'un service, et, en miroir, que les opérateurs ne sauraient exploiter pour financer leur service. Mais cette conception n'a pas été consacrée par le législateur européen, qui a privilégié le renforcement des droits des personnes concernées et la responsabilisation des responsables de traitement sur des

[19] Pratique qui peut aussi bien reposer sur des cookies que sur la fourniture directe de données personnelles par l'utilisateur du service, par le renseignement d'un formulaire d'inscription par exemple.
[20] Etant rappelé que, dans le cas particulier des cookies régis par la directive ePrivacy, le consentement n'est tout simplement pas requis pour des opérations strictement nécessaires à la fourniture d'un service demandé par l'utilisateur.
[21] L'article 7 § 4 ainsi interprété n'aurait en tous les cas de portée qu'en ce qui concerne le traitement des données dites sensibles, pour lesquelles l'exception contractuelle n'existe pas (art. 9 du RGPD).
[22] Lignes directrices sur le consentement, WP 259, p. 9.
[23] Avis n° 1/2017 (WP 247) du 4 avril 2017 sur la proposition de règlement ePrivacy.
[24] Avis 04/2017 du 14 mars 2017 sur le projet de règlement ePrivacy (pt. 62).

prohibitions de principe. Vous observerez que ce qu'on appelle parfois le « troc 2.0 » est au contraire expressément admis par la directive 2019/770 du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques (considérant 24 et articles 2 et 3).

Comme l'a déjà jugé la Cour de cassation italienne[25] et la Haute cour de Francfort[26], et comme l'a estimé l'avocat général devant la Cour de justice dans l'affaire ayant donné lieu à l'arrêt du 1er octobre 2019 déjà évoqué[27], **le RGPD ne comporte ni n'implique aucune interdiction générale et absolue[28] de la pratique du couplage**, contrairement à ce que souhaitait le Parlement européen en 1ère lecture[29]. Cette problématique n'est pas sans rappeler, d'ailleurs, l'absence d'interdiction de principe des ventes liées en droit commercial européen et l'exigence d'une recherche au cas par cas d'une éventuelle atteinte au consentement libre et éclairé du consommateur[30].

Notre conviction est que cette question appelle une analyse casuistique, permettant d'apprécier l'incidence d'un *cookie wall* déterminé sur la situation concrète d'une personne concernée.

C'est ainsi que nous comprenons le considérant 42 du RGDP[31], qui lui non plus ne trouve pas d'écho dans le corps du texte, et qui énonce que « *le consentement ne devrait pas être*

[25] V. son arrêt du 2 juillet 2018 (n° 17278).
[26] Dans un jugement du 27 juin 2019.
[27] M. Szpunar y évoque une règle d'« *interdiction de lier les consentements* » **dépourvue de caractère absolu** (pts. 97-98). Il estimait que les traitements de données personnelles en cause dans l'affaire Planet49 (installation de cookies et réception d'offres promotionnelles de diverses sociétés) pouvaient être regardés comme nécessaires à la participation au jeu promotionnel, dès lors que la fourniture de ces données constitue l'obligation principale.
[28] L'arrêt de la Cour suprême autrichienne du 30 août 2018 qui retient une telle prohibition est erroné car fondé sur la version allemande du considérant 43 du RGPD, qui n'évoque pas une présomption mais, en raison d'une erreur de traduction, une interdiction de principe, contrairement aux autres versions linguistiques.
[29] V. T7-0212/2014, paragraphe 4 de l'article 7 : « (...) *l'exécution d'un contrat ou la fourniture d'un service n'est pas soumise à la condition préalable du consentement au traitement des données qui ne sont pas nécessaires à l'exécution du contrat ou à la fourniture du service, en vertu de l'article 6, paragraphe 1, point b)* ».
[30] La directive 2005/29/CE du Parlement européen et du Conseil, du 11 mai 2005, relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur a mis fin à l'interdiction de principe des ventes liées pour ne condamner que celles qui constituent des pratiques déloyales, soit parce qu'elles sont trompeuses en raison des biais d'information du consommateur, soit parce qu'elles sont agressives, soit encore parce qu'elles sont contraires à la diligence professionnelle et sont susceptibles de provoquer une altération substantielle du comportement économique du consommateur moyen (définie par le e) de l'article 2 de la directive comme « *l'utilisation d'une pratique commerciale compromettant sensiblement l'aptitude du consommateur à prendre une décision en connaissance de cause et l'amenant par conséquent à prendre une décision commerciale qu'il n'aurait pas prise autrement* »). On retrouve l'idée d'un consentement libre et éclairé.
[31] Les lignes directrices du G29 sur le consentement en font une règle posée par le RGPD lui-même, et l'interprète comme invalidant le consentement « *si la personne concernée n'est pas véritablement en mesure d'exercer un choix, se sent contrainte de consentir ou subira des conséquences négatives importantes si elle ne donne pas son consentement* ». On notera que tant la proposition initiale de la Commission que la version du RGPD adoptée par le Parlement européen en première lecture posaient la règle de l'absence de consentement valide si la personne ne dispose pas d'une véritable liberté de choix et n'est, « *dès lors* », pas en mesure de refuser ou de se rétracter sans subir de préjudice. C'est le Conseil qui en a fait deux hypothèses alternatives tout en adoptant une rédaction moins prescriptive, sans qu'on mesure bien la portée de ces deux modifications.

considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice »[32].

L'erreur de perspective que commet la CNIL, après le CEPD, tient, à notre avis, à ce qu'elle se contente d'apprécier la liberté de choix et l'existence d'un préjudice à l'échelle du site auquel l'utilisateur s'est connecté, comme si l'accès à ce site-là, quel qu'il soit, constituait un droit garanti par une norme supérieure, une sorte de droit absolu et inconditionnel d'accéder aux contenus en ligne inspiré de la « neutralité du Net ». C'est d'ailleurs la raison pour laquelle le CEPD a admis que le consentement peut être librement donné lorsque le même éditeur propose un service équivalent à celui qui est conditionné à l'utilisation de données à des fins publicitaires, par exemple un service donnant lieu au versement d'un tarif raisonnable. Mais indépendamment de cette liberté de choix interne au site, le fait de ne pas pouvoir bénéficier d'un service de communication en ligne peut n'affecter que très marginalement la liberté de choix et ne causer qu'un préjudice négligeable, pour ne pas dire inexistant dans certains cas. Or un petit désagrément, ou une opportunité manquée, n'est pas un préjudice.

La clé nous paraît résider dans la nature du besoin que l'utilisateur cherche à satisfaire et, surtout, dans **l'existence, la disponibilité et l'accessibilité d'alternatives raisonnables permettant d'atteindre un résultat équivalent**. C'est la position de la Cour de cassation italienne que nous évoquions. Le G29 ne disait d'ailleurs pas autre chose dans un document de travail de 2013 consacré spécifiquement aux cookies[33], qui nous convainc bien plus que ces réflexions postérieures[34]. Telle était aussi l'opinion du contrôleur européen de la

---

[32] Selon les lignes directrices du G29 sur le consentement, endossées par le CEPD, il y a « préjudice » au sens du considérant 42 en cas de frais financiers, de désavantage évident, de tromperie, d'intimidation, de coercition ou de « *toute conséquence négative importante* », notamment une qualité de service amoindrie. Mais elles précisent aussi que le RGPD « *n'exclut pas tous les incitants* ».

[33] Document de travail n° 02/2013 énonçant des lignes directrices sur le recueil du consentement pour le dépôt de cookies, 2 octobre 2013 (WP 208), p. 7 : « *Si certains cookies ne sont, dès lors, pas nécessaires au regard de la finalité de la fourniture du service par le site web, mais se bornent à offrir des avantages supplémentaires à l'opérateur du site web, l'utilisateur devrait se voir offrir un choix véritable en ce qui concerne ces cookies. Les types de cookies susceptibles d'être disproportionnés au regard de la finalité du site web peuvent varier en fonction du contexte. Un exemple dans lequel il serait considéré comme disproportionné de solliciter le consentement pour des cookies superflus sont les sites web offrant certains services, dont on peut considérer que l'utilisateur n'a que peu de possibilités, voire n'a pas d'autre possibilité que d'utiliser ces services, de sorte qu'il n'est pas véritablement en mesure d'exercer un choix quant à l'usage de cookies. Dans la plupart des États membres de l'UE, cela s'applique particulièrement aux services du secteur public* » (il y est précisé en note de bas de page 11 que « *dans la grande majorité des États membres de l'UE, il n'est pas légal de rendre conditionnel l'accès à des sites web de service public* »). En s'appuyant sur la lettre du considérant 25 de la directive de 2002, le même document distingue toutefois le *cookie wall* général (permettant de refuser l'accès à l'ensemble du site), qui ne devrait pas être admis, et le *cookie wall* spécifique (permettant de refuser l'accès à certains contenus), admissible dans son principe.

[34] Il y a lieu d'observer que l'une des dernières versions du projet de règlement ePrivacy (12293/19, 18 septembre 2019) comporte un considérant qui fait justement de l'éventail de choix s'offrant à l'internaute le critère central de licéité des *cookie walls* - choix au sein des différentes offres d'un même fournisseur (dans ce cas, il y aurait présomption de licéité) ou entre les offres de différents fournisseurs (le texte indiquant que, dans certains cas, notamment celui dans lequel l'utilisateur n'a pas ou peu d'autres options que de visiter un site donné, notamment celui d'une autorité publique, le consentement ne serait pas considéré comme libre). Ce texte

protection des données dans l'avis déjà mentionné (pt. 60). On trouve également plusieurs jalons doctrinaux sérieux en ce sens[35]. Dans cet exercice d'analyse, il y a aussi lieu de prendre en compte, conformément au considérant 43 de la directive et par analogie avec les clauses abusives des contrats de consommation[36] et les vices du consentement régis par l'article 1143 du code civil[37], l'existence éventuelle d'un « *déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière* ».

S'agissant de services administratifs, par exemple l'accès à une téléprocédure, le monopole de l'administration et l'absence d'équivalence ergonomique du déplacement au « guichet » doivent conduire à proscrire résolument les *cookie walls*[38]. S'agissant de services commerciaux concurrentiels[39], l'existence d'un choix réel entre plusieurs sites, dont certains ne pratiquent pas le couplage ou admettent le découplage par des accès tarifés, devrait en général conduire à la conclusion inverse, sous réserve notamment de la position dominante d'un acteur qui pourrait le contraindre, pour prévenir tout abus, à ne pas recourir aux *cookie walls*[40]. L'appauvrissement potentiel de l'offre en ligne disponible ne constitue pas un « préjudice ». La difficulté est plus sérieuse lorsque tous les services concurrents pratiquent le

---

a été rejeté par le COREPER. La dernière version en date, proposée par la présidence croate (5979/20 du 21 février 2020), se place sur un terrain différent, consistant à permettre le dépôt et la lecture des cookies si la balance des intérêts est favorable à l'opérateur (sur celui de la personne concernée). A ce titre, elle inclut les cookies destinés à financer un service sauvegardant la liberté d'expression et d'information, notamment la presse en ligne (V. projet de considérant 21b) mais exclut les cookies à des fins de profilage, et n'apporte pas de précision sur la possibilité de recourir au consentement.

[35] V. pour une étude approfondie de la question, B. Kostic et Emmanuel Vargas Penagos, *The freely given consent and the « bundling » provision*, Computerrecht 2017/153, spécialement les exemples 3.1. et 3.2. V. aussi l'intéressant article de V. Treitl, *The coupling ban in data protection law – A first approach*, publié sur Internet.

[36] L'article L. 212-1 du code de la consommation prohibe les clauses abusives en raison du déséquilibre significatif entre les droits et obligations respectifs du professionnel et du consommateur. A notre connaissance, aucune juridiction n'a qualifié d'abusive une clause de conditions générales d'utilisation d'un service en ligne prévoyant la collecte et l'utilisation de données personnelles fournies par l'utilisateur à des fins publicitaires (V. en particulier les jugements rendus par le TGI de Paris concernant Twitter, Google et Facebook). La Commission européenne et la DGCCRF se sont au contraire félicitées, l'année dernière, que Facebook clarifie ses conditions générales d'utilisation, que l'utilisateur est tenu d'accepter s'il souhaite accéder au service, en l'informant clairement de ce que ses données sont exploitées à des fins de ciblage publicitaire (V. le communiqué de presse de la DGCCRF du 10 avril 2019).

[37] L'article 1143 du code civil qualifie de vice du consentement, au titre de la violence, le fait pour une partie d'abuser de « *l'état de dépendance dans lequel se trouve son cocontractant à son égard pour obtenir de lui un engagement qu'il n'aurait pas souscrit en l'absence d'une telle contrainte et en tire un avantage manifestement excessif* ».

[38] La version du RGPD adoptée par le Parlement européen en première lecture illustrait ainsi le cas dans lequel la personne concernée ne dispose pas d'une véritable liberté de choix en citant le traitement d'une autorité publique qui peut, en vertu de ses prérogatives de puissance publique, imposer une obligation (considérant 33).

[39] On voit bien que la pression concurrentielle constitue un puissant facteur de régulation du recours aux cookie walls. Un acteur du e-commerce, par exemple, hésitera à y recourir de crainte de se priver d'une clientèle potentielle soucieuse de protéger ses données personnelles. De manière générale, chaque éditeur de site est amené à arbitrer entre la maximisation de son audience et la valorisation des données personnelles des visiteurs.

[40] V. à cet égard l'intéressante décision de l'Autorité de la concurrence allemande de février 2019 à propos de Facebook.

couplage, même si la liberté de choix ne disparaît pas totalement. Outre la renonciation pure et simple à un service en ligne, au profit par exemple d'un recours au papier – par exemple, l'abonnement à un journal papier - l'utilisateur peut encore choisir celui des opérateurs auquel il accepte d'accorder sa confiance, en fonction des finalités poursuivies par le traitement et des engagements qu'il prend en matière de protection des données personnelles. Vous noterez que, s'agissant des ventes liées, la Cour de justice de l'Union européenne ne semble pas faire de l'effectivité d'un choix alternatif une condition de licéité de cette pratique commerciale[41].

Naturellement, la situation particulière dans laquelle se trouve la personne concernée peut affecter sa liberté de choix, même en présence d'alternatives sur le marché. On ne peut probablement pas traiter de la même façon le refus de consentement *ab initio* et le retrait du consentement lorsqu'une relation contractuelle est déjà engagée. Il faut aussi tenir compte de la difficulté éventuelle à changer d'opérateur et d'effets de réseaux inhérents à certains services en ligne[42].

Au fond, ce qu'on discerne à travers l'extrême diversité des situations, c'est qu'il est hasardeux d'asséner que les personnes dûment éclairées sur les conséquences de leurs actes seraient toujours privées de leur liberté de consentir face à un *cookie wall*, comme si les internautes étaient tous des majeurs incapables. C'est à travers la plainte d'une personne qui estime avoir été contrainte de fait de consentir que peut s'enclencher un débat sur l'éventuelle privation de liberté. La sienne.

En posant en principe, à peine de sanction[43], que la personne concernée, quelle que soit sa situation, ne peut jamais donner un consentement libre à l'utilisation de ses données à

---

[41] D'une part, « *une pratique commerciale consistant en la vente d'un ordinateur équipé de logiciels préinstallés sans possibilité pour le consommateur de se procurer le même modèle d'ordinateur non équipé de logiciels préinstallés ne constitue pas, en tant que telle, une pratique commerciale déloyale au sens de l'article 5, paragraphe 2, de la directive 2005/29* » (CJUE, 7 septembre 2016, *D…-B… c/ Sony Europe Limited*, C-310/15, pt. 42 ; G. Loiseau, *La saga du plug and play touche à sa fin*, Communication Commerce électronique, n° 10, octobre 2016, comm. 81 : « *L'impression d'ensemble est que la position de la Cour de justice est moins exigeante que celle de la Cour de cassation. Contrairement à la seconde, la première ne conditionne pas l'absence de pratique déloyale à une possibilité de choix pour les clients qui doivent disposer d'une formule alternative portant sur la seule partie hardware. Pour la Cour de Bruxelles, les appareils peuvent être commercialisés uniquement avec les logiciels* (...) ». D'autre part, l'arrêt renvoie à la juridiction nationale le soin de déterminer si le consommateur a été, en l'espèce, apte à prendre une décision commerciale en connaissance de cause, dans le cas où il a été « *dûment informé, avant de procéder à l'achat, que le modèle d'ordinateur faisant l'objet de la vente n'était pas commercialisé sans logiciels préinstallés et qu'il était, de ce fait, en principe libre de choisir un autre modèle d'ordinateur, d'une autre marque, pourvu de caractéristiques techniques comparables, vendu sans logiciels ou associé à d'autres logiciels* » (pt. 41). Ce « en principe » pourrait signifier qu'il n'y a pas lieu d'examiner concrètement s'il existe une alternative disponible sur le marché.

[42] Même si le RGPD offre lui-même des facilités, à travers le droit à la portabilité des données en particulier, il existe parfois des effets de réseaux qui peuvent dissuader une personne de changer d'opérateur – c'est le cas des réseaux sociaux.

[43] A cet égard, nous pensons que la très grande imprécision du droit de l'Union sur la question devrait, au titre du principe de légalité des délits, faire obstacle à l'infliction de sanctions pour ce motif, en tous les cas aussi longtemps que la Cour de justice n'a pas clarifié la portée de la directive ePrivacy à cet égard. Il nous paraît conceptuellement très difficile de concilier l'exigence de prévisibilité de la loi répressive et l'existence d'une difficulté sérieuse justifiant une clarification de la Cour de justice. Mais nous reconnaissons qu'une telle construction mériterait une formation supérieure de jugement...

caractère personnel lorsque le responsable de traitement subordonne l'accès à un site Internet ou un service de communication en ligne, quel qu'il soit, à un tel traitement, quelles que soient les conséquences concrètes du refus de consentir, la CNIL nous parait donc avoir méconnu l'article 82 de la loi du 6 janvier 1978 et le RGPD.

Vous pourriez légitimement hésiter à prendre une position aussi ferme sur l'interprétation du RGPD sans l'aval de la Cour de justice. Aussi pourriez-vous préférer, alternativement, juger plus discrètement qu'il n'appartenait pas à la CNIL, dans le cadre d'un acte de droit souple tel que celui en litige, de poser une interdiction générale et absolue qui ne ressort d'aucun texte en vigueur. Une telle interdiction, très attentatoire à la liberté contractuelle et à la liberté d'entreprendre, ne pourrait résulter que d'une législation – européenne ou nationale – explicitement en ce sens, ce d'autant plus que la méconnaissance de la règle du consentement est passible non seulement de sanctions administratives qui peuvent atteindre 4% du chiffre d'affaires annuel mondial, mais aussi, lorsque sont en cause des données à caractère personnel, de sanctions pénales puisque l'article 226-18 du code pénal punit de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait de collecter de telles données de manière déloyale ou illicite. Ce texte clair est celui que le CEPD appelle de ses vœux, à savoir un règlement ePrivacy qui interdirait expressément les *cookie walls*. Mais justement, cette réforme fait l'objet de profonds désaccords entre Etats membres[44], notamment sur cette question précise, ce qui augure d'ailleurs mal du devenir de ce texte. **Il n'appartient ni à la CNIL, ni au juge de prendre la plume à la place du législateur européen.** Précisons que ce terrain alternatif ne diffère guère, au fond, du précédent. Si vous considériez que le RGPD prohibait les *cookie walls*, alors rien n'interdirait à la CNIL de le rappeler dans un acte de droit souple. Comme en matière de circulaire, la compétence et le fond sont intimement liés.

Au total, la Commission aurait dû, plus prudemment, se contenter de recommander aux opérateurs de s'abstenir de se livrer à des pratiques de couplage, dès lors qu'elle les considérait comme contraires à l'esprit du RGPD.

Nous vous proposons donc de censurer le 4ème alinéa de l'article 2 des lignes directrices, qui est divisible et laissera simplement subsister le rappel de la position du CEPD.

*

Les requérants s'en prennent ensuite à l'exigence, figurant au 7ème alinéa du même article 2, que la personne concernée puisse **donner son consentement de façon indépendante et spécifique pour chaque finalité distincte** pour laquelle des cookies sont déposés ou lus. De leurs écritures évolutives, on comprend qu'ils contestent à la fois le principe « une finalité, un consentement propre », plaidant à cet égard pour qu'il soit possible de ne prévoir qu'un consentement global, et qu'ils revendiquent la possibilité de pouvoir utiliser les données collectées à partir des cookies pour des finalités autres que celles ayant justifié cette collecte, pourvu que ces finalités soient compatibles avec les finalités initiales du traitement.

[44] Une présentation de la Commission européenne annexée à un document de travail du Conseil (WK1118/2020 INIT) du 30 janvier 2020 indique que 18 Etats membres sur 27 ont émis le souhait que la notion de consentement soit clarifiée dans le cadre de la directive ePrivacy.

Le premier point critiqué, qui est conforme aux lignes directrices du CEPD sur le consentement[45], soulève un débat de principe qui, à nos yeux, est plus délicat encore que le précédent. L'article 4 du RGPD, qui définit le consentement, exige que la manifestation de volonté soit « spécifique ». Mais contrairement à ce qu'indique le CEPD depuis la deuxième version des lignes directrices, nous ne pensons pas que cette exigence implique une granularité du consentement au niveau de la finalité. Elle signifie seulement que le consentement à un traitement de données à caractère personnel doit être recueilli de manière distincte du consentement à d'autres obligations ayant un objet différent. C'est ce que juge la Cour de justice au point 58 de son arrêt *Planet49* du 1er octobre 2019 (C-673/17), aussi bien sur le fondement de la directive de 1995 que sur celui du RGPD[46]. Cette exigence s'oppose ainsi à la pratique consistant à souscrire de manière globale à des conditions générales de vente d'un produit ou d'utilisation d'un service qui comprennent, entre autres, la mise en œuvre d'un tel traitement, ce que rappellent à juste titre les lignes directrices litigieuses[47].

De même, à la lettre, le paragraphe 1, sous a), de l'article 6 du RGPD, éclairé par son considérant 32, exige seulement que le consentement à un traitement poursuivant plusieurs finalités spécifiques[48] porte sur l'ensemble de ces finalités, et non sur chacune d'entre elles[49] –

---

[45] Lignes directrices, p. 14 : « *Cela signifie qu'un responsable du traitement qui sollicite le consentement pour diverses finalités spécifiques devrait prévoir un consentement distinct pour chaque finalité afin que les utilisateurs puissent donner un consentement spécifique à des finalités spécifiques* ».

[46] « *Il convient d'ajouter que la manifestation de volonté visée à l'article 2, sous h), de la directive 95/46 doit, notamment, être « spécifique », en ce sens qu'elle doit porter précisément sur le traitement de données concerné et ne saurait être déduite d'une manifestation de volonté ayant un objet distinct* ».

[47] Le paragraphe 2 de son article 7 fixe par ailleurs des règles formelles permettant de bien distinguer cette demande de consentement spécifique. Cette exigence de consentement spécifique existe aussi en matière de prospection commerciale et vous l'avez interprétée comme un consentement distinct de celui donné aux conditions générales d'utilisation d'un logiciel (CE, 11 mars 2015, *Sté TUTO4PC*, n° 368624, aux T.). Mais dans ce précédent, le traitement n'avait qu'une seule finalité, à savoir la prospection commerciale. On relèvera toutefois que l'obligation de consentement préalable à ce type de traitements a été instituée à l'origine par la directive ePrivacy de 2002, alors que la directive 95/46 exigeait déjà un consentement « spécifique » à tout traitement de données à caractère personnel. On pourrait y voir un indice (faible) de ce que cette directive n'imposait pas un consentement par finalité et qu'il était nécessaire de l'instituer pour la prospection commerciale.

[48] On peine à comprendre la portée exacte de l'expression « finalité(s) spécifique(s) » utilisée à six reprises par le RGPD et qui était ignorée de la directive 95/46. Sur ce plan, le règlement paraît empreint d'une certaine iprécision terminologique. A titre d'exemple, le b) du paragraphe 1 de l'article 5 exige que les données à caractère personnel soient collectées pour des « *finalités déterminées, explicites et légitimes* » ; or le considérant 39 qui explicite ces dispositions dispose quant à lui que : « *les finalités spécifiques du traitement* (...) *devraient être explicites et légitimes, et déterminées lors de la collecte des données* (...) ». Le considérant 42 qui traite du consentement subordonne le caractère éclairé du consentement à la condition d'informer la personne de l'identité du responsable du traitement et des « finalités du traitement », sans préciser qu'elles doivent être « spécifiques ». Nous comprenons que cette expression n'a qu'une portée limitée. Elle signifie « finalités précises » ; elle prohibe ainsi les formulations trop vagues, et une globalisation excessive des finalités (i.e : « catégories de finalités » trop larges). La proposition initiale de la Commission (pt. 3.4.2) indiquait reprendre les bases légales issues de la directive 95/46, sous réserve de précisions sur certaines bases légales – mais pas celle du consentement – et l'exposé des motifs du Conseil en première lecture semble indiquer que les bases juridiques prévues par la directive 95/46 ont été reprises telles quelles, en substance (p. 8 : « *Par rapport à la directive 95/46/CE, le*

subtilité sémantique qu'on retrouve dans d'autres versions linguistiques du règlement[50]. Cela signifie qu'un traitement ne peut être mis en œuvre pour une finalité donnée si le consentement de la personne concernée n'a pas porté sur cette finalité, sans préjudice de la mobilisation d'une autre base légale prévue à l'article 6.

Il est certain en revanche que, comme pour les *cookie walls*, le couplage des finalités peut affecter le **caractère libre du consentement**, ce qu'indiquent les mêmes lignes directrices du CEPD depuis l'origine. C'est ce qui ressort là encore du considérant 43 du RGPD, selon lequel le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à « *différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce* », même si, une fois de plus, aucun article du RGPD ne s'en fait l'écho[51]. Il conviendrait alors d'analyser au cas par cas dans quelle mesure l'assentiment de la personne à une finalité a été abusivement « arraché » par le recueil d'un consentement global.

Un autre raisonnement consisterait à considérer qu'il existe autant de traitements de données que de « catégories homogènes de finalités »[52]. Certes, les termes mêmes du RGPD impliquent qu'un même traitement puisse avoir plusieurs finalités et, comme on vient de le dire, il n'exige pas explicitement le recueil de plusieurs consentements par traitement. Mais cela n'interdit pas de bâtir un raisonnement fondé sur la connexité[53] ou, pour reprendre un

---

règlement assure, pour l'essentiel, une continuité au regard des principes sous-tendant le traitement de données à caractère personnel (…) *En vue de garantir la sécurité juridique, la position du Conseil en première lecture s'appuie sur la directive 95/46/CE pour préciser que le traitement de données à caractère personnel n'est licite que si au moins une des conditions suivantes est remplie: / - la personne concernée a consenti au traitement pour une ou plusieurs finalités spécifiques* (…) »).

[49] Le Manuel de droit européen en matière de protection des données lit ce considérant comme exigeant un consentement par finalité (p. 164).

[50] « *All of them* » (purposes) et non « *each one of them* » ou encore « *alle* » (Verarbeitungszwecke) et non « *jede* » Cette rédaction est issue des travaux du Conseil en première lecture, sans que l'exposé des motifs ne l'explicite davantage qu'en paraphrasant le texte.

[51] L'ICO britannique fonde la granularité du consentement au niveau de la finalité sur ce considérant 43, tout en ouvrant la porte à une dérogation : « *The purposes of the processing : recital 43 says separate consent will be needed for different processing operations wherever appropriate – so you need to give granular options to consent separately to separate purposes, unless this would be unduly disruptive or confusing* » (excessivement perturbateur ou susceptible d'induire en erreur).

[52] Vous avez récemment rappelé que le droit à la protection des données à caractère personnel était structuré par cette notion de finalité, ce qui peut conduire à isoler un traitement réalisé à partir d'un fichier pour lui appliquer le cadre juridique pertinent au regard de sa finalité propre, distinct de celle pour laquelle ce fichier a été initialement constitué (CE, 27 mars 2020, *Association CRPA et autres*, n° 431350 et a., aux T. à propos du fichier HOPSYWEB). De ce point de vue, la granularité par finalité se distingue clairement d'autres dimensions, comme, par exemple, la granularité par catégories de destinataires (« *je consens à ce que mes coordonnées soient communiquées à tel ou tel partenaire commercial du responsable de traitement, mais pas à tel autre* »). Pour l'application de l'article 12 de la directive ePrivacy, et avant le RGPD, la CJUE a par exemple admis que les données d'abonnés au téléphone soient transmises à des entreprises autres que leur opérateur téléphonique dès lors que les traitements mis en œuvre poursuivent la même finalité (CJCE, 5 mai 2011, *Deutsche Telekom AG*, C-543/09, pt. 65). Il est certain que, si le RGPD entend renforcer la maîtrise de leurs données par les personnes concernées, on ne peut admettre un consentement totalement à la carte, qui reviendrait indirectement à confier aux personnes le droit de modifier les caractéristiques du traitement.

vocable utilisé par le RGPD, la compatibilité des finalités[54] afin de distinguer le cas d'un authentique traitement pluri-finalités, qui appellerait un unique consentement, et celui où, derrière la diversité des finalités, se cachent en réalité des traitements distincts, appelant des consentements distincts[55].

A l'évidence, seule la Cour de justice pourrait élaborer une doctrine d'emploi complète de ces dispositions. Nous pensons toutefois que vous pouvez faire l'économie d'une question préjudicielle dans le présent dossier, en vous appuyant sur le **régime juridique propre aux cookies, tel que défini par le législateur national**. Là où le paragraphe 3 de l'article 5 de la directive ePrivacy exige une information et un accord de l'internaute sur « les finalités » du dépôt et de la lecture de cookies, l'article 82 de la loi de 1978 impose une information, et par conséquent un consentement, sur « *la finalité de toute action* » tendant à accéder à des informations stockées dans le terminal ou à y inscrire des informations. Le législateur a donc exigé, pour ces opérations intrusives, que l'information comme le consentement porte sur chaque finalité, de sorte qu'une personne doit pouvoir accepter le dépôt et l'utilisation de cookies pour une finalité et les refuser pour une autre. Cela n'empêche évidemment que, pour des raisons d'ergonomie, l'éditeur du site donne la possibilité à l'internaute d'approuver simultanément l'ensemble des finalités présentées, en cochant une case à cet effet, quitte ensuite à « décocher » celles qui ne lui conviennent pas.

Sur le second point critiqué, il est certain que l'article 5 et le paragraphe 4 de l'article 6 du RGPD autorisent des traitements ultérieurs qui peuvent ne pas reposer sur le consentement des personnes concernées mais relever de l'une des autres bases juridiques énumérées à cet article 6, pourvu qu'ils poursuivent des finalités compatibles avec la ou les finalités d'origine. Il en va ainsi quand bien même le traitement d'origine reposerait sur le consentement de la personne[56]. Mais l'acte attaqué ne prend pas parti sur ce point, de sorte que la critique manque

---

[53] Dans l'avis 03/2013 du 2 avril 2013 sur la limitation des finalités, le G29 admettait que, pour des opérations de traitement suffisamment liées, il soit fait été d'une finalité chapeau (V. p. 16).

[54] Dans son avis 15/2011 du 13 juillet 2011 sur la définition du consentement, le G29 recourait au critère des « attentes raisonnables » des utilisateurs (« *En principe, il devrait suffire que les responsables du traitement obtiennent un consentement unique pour les différentes opérations, si celles-ci relèvent des attentes raisonnables de la personne concernée* »). Or ce critère est aussi utilisé pour déterminer la compatibilité d'une finalité additionnelle avec une finalité originelle.

[55] Il y aurait une grande cohérence logique avec l'encadrement des traitements ultérieurs. Le paragraphe 4 de l'article 6 du RGPD permet en effet à un responsable de traitement de traiter des données initialement recueillies pour une finalité A afin de poursuivre une finalité B dès lors, d'une part, que B est compatible avec A – le RGPD fournit sur ce point une liste de critères pour apprécier la compatibilité – et, d'autre part, qu'une base légale autre que le consentement peut jouer, en particulier le cas où l'intérêt légitime du responsable prévaut sur les intérêts des personnes concernées. On ne voit pas bien pourquoi on exigerait un consentement portant sur A et B alors que la finalité B pourrait être ultérieurement poursuivie sans le consentement de la personne. Pour reprendre l'exemple d'HOPSYWEB, il est clair que la finalité « suivi administratif des patients » était incompatible, au sens du RGPD, avec la finalité « suivi des radicalisés ». Si la base légale avait été le consentement, il aurait fallu recueillir des consentements distincts. A l'inverse, la finalité « réalisation de statistiques » ne nous paraît pas nécessiter un consentement individualisé, les traitements ultérieurs à des fins statistiques étant présumés compatibles avec les finalités d'origine du traitement (considérant 50 du RGPD).

[56] Le considérant 50 du RGPD ne fait pas de distinction à cet égard. En outre, si les lignes directrices du G29 sur

sa cible. En tout état de cause, l'article 82 de la loi de 1978, comme le paragraphe 3 de l'article 5 de la directive ePrivacy, exclut toute autre base juridique que le consentement. Il neutralise donc la possibilité offerte par le RGPD de réutiliser des données personnelles issues de la lecture des cookies pour des finalités non dévoilées à l'internaute et auxquelles ce dernier n'aurait donc pas consenti.

*

Le grief suivant s'adresse aux esprits subtils. Il vise le dernier alinéa de l'article 2 des lignes directrices, placé sous le chapeau « *Retrait du consentement* », mais où la CNIL glisse l'idée que : « *il doit être aussi facile de refuser ou de retirer son consentement que de le donner* »[57].

Cette précision peut sembler incongrue puisque, dans un régime d'*opt-in*, tant qu'on ne clique pas sur « *Accepter* », on refuse, y compris, vous l'avez rappelé l'année dernière, si on continue à naviguer au sein de la page ou du site. L'enjeu est toutefois loin d'être anecdotique, y compris sur le plan économique, car, à défaut de pouvoir refuser expressément et facilement, la tentation est grande pour l'internaute moyen d'accepter pour se débarrasser d'un bandeau gênant, plutôt que de devoir cliquer sur les décourageants « *En savoir plus* », « *Plus d'options* » ou encore « *Paramétrer les cookies* ».

Nous relevons que le 2° de l'article 82 de la loi de 1978 fait obligation au responsable de traitement d'informer l'utilisateur des moyens de s'opposer aux opérations de dépôt et de lecture. Qu'elle soit ou non une scorie datant du temps de l'*opt-out*, cette disposition existe et confirme que l'utilisateur doit pouvoir refuser expressément ces traitements. Elle fait du reste écho au considérant 66 de la directive de 2009 qui évoque un « *droit de refus* » alors même que cette directive institue un mécanisme de consentement préalable.

Les requérantes ne le contestent pas frontalement mais voient dans la formulation litigieuse une obligation de faire figurer sur chaque site, voire sur chaque page du site, un bouton « *Refuser les cookies* ».

Comme l'indique la CNIL, les lignes directrices attaquées n'imposent aucune modalité technique de recueil de ce refus. Elles se bornent à exiger, de manière générale et à juste titre, qu'il ne soit pas plus compliqué de refuser que d'accepter. Elles s'accommodent implicitement d'une solution qui consisterait à ne pas offrir de bouton « je refuse », pour autant que le simple fait de fermer le bandeau, en cliquant classiquement sur une croix située en haut à droite, celui de changer de page voire celui de parcourir la même page pendant un

---

le consentement exigent qu'un nouveau consentement soit recueilli préalablement à la mise en œuvre d'un traitement ayant une autre finalité que celle pour laquelle la personne concernée avait donné son consentement initial, cette analyse réserve précisément le cas des traitements compatibles (« *sans préjudice des dispositions relatives à la compatibilité des finalités*... »).

[57] Le paragraphe 3 de l'article 7 du RGPD prévoit seulement qu'il est « *aussi simple de retirer que de donner son consentement* », sans évoquer le refus.

laps de temps déterminé vaille refus et que l'internaute ne soit pas pourchassé de page en page par des demandes de consentement ou gêné par des artifices d'affichage affectant l'ergonomie de la navigation.

La requête aborde également le sujet délicat de la possibilité pour l'éditeur du site de re-solliciter ultérieurement l'accord de l'internaute qui a antérieurement manifesté son refus, explicitement ou implicitement. Mais là encore, la délibération litigieuse n'en dit rien. Contrairement à ce qui est soutenu, elle ne traite pas de la question de la « durée de validité du refus » ou de la « durée de conservation des traces du refus ».

Nous vous proposons de laisser ce débat de fond à l'éventuelle contestation de la future recommandation, qui prendra clairement parti sur ce point, selon la CNIL.

*

Les requérants s'en prennent ensuite au paragraphe relatif au caractère éclairé du consentement, dont il ressort que l'utilisateur doit être informé de l'identité du ou des responsables de traitement préalablement au dépôt ou à la lecture de cookies et qu'il doit pouvoir identifier « *l'ensemble des entités ayant recours à des traceurs* » avant de pouvoir y consentir, ce qui suppose que la liste exhaustive et régulièrement mise à jour de ces entités soit mise directement à sa disposition lors du recueil de son consentement.

Toute personne qui réalise des opérations de dépôt ou de lecture de cookies pour son propre compte en est le **responsable de traitement**. Il peut s'agir de l'éditeur du site lui-même, le cas échéant avec l'aide d'un sous-traitant, ou d'un opérateur tiers avec l'autorisation de l'éditeur du site visité[58]. Dans ce dernier cas, vous avez jugé que l'éditeur devait aussi se voir reconnaître cette qualité (CE, 6 juin 2018, *Société Editions Croque Futur,* n° 412589, au Rec.)[59]. Les personnes qui obtiennent, en seconde main, la communication de données issues de ces opérations de lecture de la part du ou des responsables de traitement ont, quant à eux, la qualité de **destinataires des données**.

Curieusement, l'article 82 de la loi de 1978 n'exige pas formellement l'indication de l'identité du ou des responsables de traitement. Mais c'est ainsi qu'il doit s'interpréter car le droit de l'Union l'impose très certainement[60]. Le paragraphe 3 de l'article 5 de la directive ePrivacy

[58] On parle parfois de « cookies tiers » à cet égard (à ne pas confondre avec les cookies tierce partie, qui sont ceux mis en place par des sites web appartenant à un domaine distinct du domaine dont relève le site web consulté par l'utilisateur tel qu'il apparaît dans la barre d'adresse du navigateur).

[59] Dans la terminologie du RGPD, il doit être considéré comme un « responsable conjoint de traitement », au sens de son article 26, même si, compte tenu de la portée limitée des obligations pesant sur lui, il serait plus pertinent d'y voir un « responsable secondaire de traitement ».

[60] L'exigence d'information sur le ou les responsables de traitement ne méconnaît en rien l'article 95 du RGPD, invoqué par la requête, qui se borne à préciser que ce règlement n'ajoute pas d'obligations supplémentaires par rapport à celles qui résultent de la directive ePrivacy en ce qui concerne les aspects pour lesquels elles sont soumises à des obligations spécifiques ayant le même objectif. Elle n'introduit par ailleurs aucune distorsion de

procède par renvoi exprès à la directive de 1995 et, désormais, au RGPD, pour la définition des informations qui doivent être fournies à l'utilisateur. Selon l'article 13 du RGPD, l'identité du ou des responsables de traitement en fait partie, de même que celle des destinataires ou catégories de destinataires des données. C'est ce qu'a rappelé la Cour de justice dans son arrêt du 1er octobre 2019 (considérant 77) en ajoutant même à la liste fixée par le RGPD toutes les informations nécessaires pour assurer à l'égard de la personne concernée un traitement loyal de ses données, comme la durée de fonctionnement des cookies[61].

Par ailleurs, l'exigence de mise à disposition d'une liste exhaustive et mise à jour des responsables de traitement découle nécessairement de l'obligation d'information posée par le RGPD, qui s'apprécie de manière dynamique, comme le rappellent les lignes directrices du CEPD sur la transparence[62].

Il est aussi reproché à la CNIL d'avoir imposé aux opérateurs de fixer une liste exhaustive des **destinataires des données** mais la Commission indique en défense qu'elle n'a pas entendu les inclure dans la notion d'« *entités ayant recours à des traceurs* »[63]. Nous vous proposons d'en prendre acte même si, comme nous l'avons dit, le RGPD exige au moins que les catégories de destinataires des données soient précisées, sans qu'il soit nécessaire, en revanche, de désigner nommément chacun d'eux[64]. Les reproches qui sont faits à la délibération à cet égard s'en trouvent en conséquence privés de portée. Nous pensons toutefois que la Commission serait bien inspirée de compléter les lignes directrices sur ce point, afin de ne pas donner une vision tronquée de la portée de l'obligation d'information pesant sur le responsable de traitement.

*

Sont ensuite en cause les « **cookies de mesure d'audience** ». La délibération rappelle que certains d'entre eux peuvent bénéficier d'une dispense de recueil du consentement à certaines conditions, notamment celle de limiter leur durée de vie à 13 mois et la durée de des données

---

concurrence avec des entreprises étrangères, toutes les entreprises réalisant des opérations de dépôt et de lecture de cookies sur le terminal d'un utilisateur se trouvant en France étant soumises aux mêmes obligations.

[61] Il n'y a pas lieu de transposer la solution qu'elle a retenue pour l'article 12 de la directive ePrivacy, concernant le consentement à la publication des coordonnées téléphoniques dans un annuaire public (CJCE, 5 mai 2011, *Deutsche Telekom AG*, C-543/09). La Cour a estimé qu'un tel consentement, attaché à la finalité, était donné sans considération de l'identité des gestionnaires d'annuaire. Mais il s'agissait d'une interprétation téléologique visant à éviter des distorsions de concurrence entre opérateurs et à rendre possible l'existence d'au moins un annuaire regroupant l'ensemble des abonnés.

[62] V. les lignes directrices du G29 endossées par le CEPD, WP260 rev. 01 du 11 avril 2018 (pp. 19-21).

[63] On notera que dans l'avis qu'elle a émis sur le projet d'ordonnance transposant la directive de 2009 modifiant la directive ePrivacy de 2002, la CNIL avait demandé, sans succès, que l'article 32 de la loi de 1978 soit complété pour ajouter cette rubrique des « destinataires ».

[64] Dans ses conclusions sur l'arrêt du 1er octobre 2019, l'avocat général Szpunar estimait que l'identité de tout tiers ayant accès aux cookies devait être divulgué. Dans l'arrêt, il est fait référence aux destinataires et catégories de destinataires. Il nous semble que l'arrêt et les conclusions ne retiennent pas la même interprétation de la notion de « tiers ayant accès aux cookies ».

qu'ils permettent de collecter à 25 mois. Vous noterez que la recommandation de 2013 comportait le même dispositif, à ceci près que la durée de conservation des données collectées était elle-même limitée à 13 mois.

Les requérants, pourtant mieux lotis que sous l'empire de cette recommandation, estiment que la CNIL ne pouvait légalement ajouter une telle condition, qui ne résulte d'aucun texte.

A dire vrai, nous pensons qu'ils sont même mieux lotis que ce que le droit autorise. On peut en effet sérieusement s'interroger, à rebours de la requête, sur le point de savoir si de tels traceurs peuvent relever de l'une ou l'autre des deux dérogations à la règle du consentement prévues à l'article 82 de la loi de 1978 – autrement dit, être nécessaires au fonctionnement du site[65] ou strictement nécessaires à la fourniture d'un service expressément demandé par l'utilisateur. Dans un avis de 2012[66], réitéré en 2016, le G29 considérait que ces cookies dits d'« analytique » ne relevaient en tant que tel d'aucune des deux dérogations admises par la directive et plaidaient, en vain à ce stade, pour l'ajout d'une exemption sur mesure dans la directive ePrivacy[67]. On peut à la limite l'admettre dans le cas, évoqué par les lignes directrices, des statistiques de fréquentation et des tests de mesures de performance qui permettent aux éditeurs de détecter des problèmes de navigation dans leur site ou leur application. C'est nettement plus douteux lorsqu'il s'agit seulement, comme l'envisage aussi le document, d'optimiser l'agencement ou les contenus du site[68].

Les requérants ne reprochent évidemment pas à la Commission d'être trop laxistes, de sorte que vous ne pouvez vous saisir de cette question de légalité. Nous vous proposons toutefois de neutraliser la doctrine qu'elle a élaborée en l'interprétant comme applicable si et pour autant que les cookies de mesures d'audience en cause relèvent, le cas échéant, de l'une ou l'autre des deux dérogations admises par l'article 82 de la loi de 1978, auxquels la CNIL ne peut légalement ajouter. La rédaction de sa délibération vous le permet.

Quant à la critique dont vous êtes saisi, nous ne la croyons pas fondée. La CNIL s'est bornée ici à édicter d'authentiques lignes directrices guidant la mise en œuvre des dérogations posées

---

[65] L'article 82 évoque les cookies ayant pour finalité de permettre ou de « faciliter » la communication électronique. Mais il convient de neutraliser ou, à tout le moins, de donner une interprétation très stricte à cette notion de « facilitation », reprise de la version initiale de la directive ePrivacy et supprimée par la directive de 2009 (à l'initiative du Parlement européen) afin de limiter la dispense de recueil du consentement aux cookies « *visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques* ». L'ordonnance de 2011 a omis d'aligner la rédaction sur celle de la directive modifiée.

[66] Avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies, adopté le 7 juin 2012 (WP 194). V. aussi Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), 19 juillet 2016, WP 240, p. 12)

[67] Ce que le projet de règlement dans son dernier état connu envisage.

[68] Précisons au passage que vous avez jugé que le fait que certains cookies ayant une finalité publicitaire soient nécessaires à la viabilité économique d'un site ne saurait conduire à les regarder comme « strictement nécessaires à la fourniture » du service de communication en ligne (CE, 8 juin 2018, *Société Editions Croque Futur*, n° 412589, au Rec.).

par le texte, et dont elle pourra et devra s'écarter au cas par cas en considération des spécificités de la situation ou de motifs d'intérêt général. Les durées qu'elle a fixées visent à contraindre les opérateurs à se réinterroger périodiquement sur le point de savoir si les cookies déposés et les informations collectées sont toujours nécessaires au fonctionnement du site ou à la fourniture d'un service demandé par l'internaute et peuvent donc toujours bénéficier d'une dérogation. La contrainte qui leur est imposée est pour le moins légère puisque ces opérateurs peuvent parfaitement, s'ils estiment relever d'un cas de dérogation, redéposer de nouveaux cookies ayant la même finalité, sans recueillir le consentement de la personne.

*

Le dernier tir vise l'article 6 des lignes directrices qui prévoit qu'afin d'assurer une transparence pleine et entière sur le dépôt et la lecture des **cookies exemptés de l'exigence de consentement préalable**, les utilisateurs doivent tout de même être informés de leur existence et de leur finalité.

La délibération relève elle-même que la loi ne prévoit pas de droit d'opposition en pareil cas. Elle ne prévoit même pas d'obligation d'information. Compte tenu de cette rédaction, et en dépit du malencontreux usage de l'indicatif présent « doivent », la CNIL nous semble ici s'en être tenue à une recommandation de bonne pratique à l'intention des opérateurs. Il ne s'agit d'ailleurs pas d'une information équivalente à celle que prévoit l'article 82 de la loi de 1978, puisqu'elle se satisfait d'une simple mention dans la politique de confidentialité de l'organisation. Aucune disposition ne fait obstacle à ce que les opérateurs soient encouragés à un tel effort de transparence, sans encourir de sanction s'ils s'en abstiennent.

PCMNC :

- **à l'annulation du 4ème alinéa de l'article 2 des « lignes directrices » ;**
- **à ce qu'une somme de 4000 euros soit mise à la charge de l'Etat au titre de l'article L. 761-1 du code de justice administrative ;**
- **et au rejet du surplus des conclusions de la requête.**