N° 429571 – Société CDiscount

10^{ème} et 9^{ème} chambres réunies

Séance du 23 novembre 2020

Lecture du 10 décembre 2020

CONCLUSIONS

M. Alexandre LALLET, rapporteur public

On ne présente pas la société Cdiscount, 2^{ème} acteur du e-commerce en France derrière Amazon, avec 9 millions de clients dits « actifs ». Comme beaucoup de ses concurrents, elle a mis en place un dispositif d'achat « en un clic » dit « paiement flash », qui permet de faire l'économie du parcours d'utilisateur classique, consistant successivement à valider le panier récapitulé, choisir l'option de livraison et procéder au paiement. L'efficacité de ce dispositif repose en grande partie sur l'enregistrement préalable du numéro de carte bancaire, de sorte que le client n'est pas amené à le re-saisir.

A la suite d'une mise en demeure de la CNIL, la société, qui avait d'abord opté pour un mécanisme d'enregistrement par défaut – c'est-à-dire en l'absence d'opposition du client (*opt-out*) – a adopté un dispositif de consentement préalable express – autrement dit, d'*opt-in*. Elle a toutefois déploré une baisse sensible de son chiffre d'affaires qu'elle a imputée à cette évolution compte tenu de la très faible proportion des clients donnant leur consentement. Assez paradoxalement, elle a pris prétexte de l'entrée en application du RGPD en 2018 pour indiquer à la CNIL qu'elle entendait en revenir à un mécanisme d'*opt-out* en se fondant sur deux bases légales alternatives au consentement prévues au paragraphe 1 de l'article 6 du règlement :

- d'une part, les nécessités de l'exécution d'un contrat, prévues au b), pour les clients ayant souscrit le service « Cdiscount à volonté » ;
- d'autre part, pour les autres clients, son intérêt légitime à proposer un parcours client fluide, intérêt qui prévaudrait selon elle sur les intérêts, les libertés et les droits fondamentaux des personnes concernées, au sens du f) du même paragraphe.

C'est dans ce contexte que la CNIL a réaffirmé, actualisé et affiné sa doctrine sur ce sujet, issue d'une délibération de 2017, en adoptant une nouvelle délibération dont la société

CDiscout a demandé la modification pour lui permettre d'enregistrer le numéro de carte bancaire dans le cadre de son dispositif de « paiement flash ». Elle vous demande d'annuler le rejet de cette demande, présentée sous la forme d'un « recours gracieux » introduit dans le délai de recours¹ sans toutefois que la société demande l'annulation de la délibération elle-même.

La recevabilité de la requête ne fait aucun doute, ne serait-ce que parce que cette recommandation, acte de droit souple, est de nature à emporter des effets notables sur le plan économique², de sorte que le refus de la modifier froisse certainement les intérêts défendus par la société.

L'article 2 de la délibération attaquée distingue schématiquement trois configurations contractuelles appelant une analyse distincte du point de vue de la licéité du traitement consistant à conserver les données relatives aux cartes de paiement pour les transactions en ligne :

- dans le cas où la personne procède simplement à un achat unique sur un site Internet, fut-ce après avoir créé un compte client, les nécessités du contrat justifient seulement la conservation du numéro de carte bancaire le temps de la transaction commerciale. La conservation du numéro de carte pour faciliter d'éventuels paiements ultérieurs, notamment pour pouvoir procéder à un achat en « un clic », requiert le consentement préalable (points 2.1 et 2.4) – sur ce point, qui est au cœur du présent litige, la CNIL n'a d'ailleurs fait que confirmer sa doctrine antérieure ;
- à l'autre extrémité, si le client a souscrit un **abonnement impliquant des paiements multiples** – par exemple, un abonnement à Netflix ou à Deezer – la conservation des données bancaires jusqu'à la résiliation de l'abonnement est justifiée par les nécessités de l'exécution du contrat (point 2.2.)³ ;
- entre ces deux configurations, la CNIL identifie, de manière innovante, une **situation intermédiaire** dans laquelle le client a souscrit à un abonnement qui n'implique pas par lui-même de paiements récurrents, mais qui donne accès à des services additionnels permettant de faciliter les achats, comme la livraison rapide ou l'accès à des ventes privées. La conservation des données bancaires ne peut dans ce cas reposer

¹ Délibération n° 2018-303 du 6 septembre 2018 qui remplace la délibération n° 2017-222 du 20 juillet 2017.

² Nous pensons même qu'elle relève de la première branche de la jurisprudence *Sté Fairvesta*, concernant les « communications interprétatives », même s'il n'est pas fait état de sanctions en cas de méconnaissance de ses dispositions.

³ Il en va de même en cas de souscription à une solution de paiement dédiée à la vente à distance (point 2.3.)

sur les nécessités de l'exécution d'un contrat. En revanche, s'il est manifeste que cet abonnement traduit l'inscription du client dans une relation commerciale régulière et une intention de procéder à des achats réguliers – ce qui ne peut se déduire ni de la seule création d'un compte client, ni même de l'inscription à un programme de fidélité, la CNIL admet que l'intérêt légitime du responsable de traitement à conserver le numéro de carte bancaire pour faciliter des paiements ultérieurs prévaut sur les droits des personnes concernées, ce qui dispense du recueil du consentement au profit d'un simple régime d'*opt-out*.

Le moyen tiré de l'incompétence de la Commission pour modifier le RGPD n'a pas de portée autonome. Si l'interprétation que donne la CNIL de l'article 6 du règlement est correcte, alors elle a pu compétemment la rappeler et l'expliquer dans le cadre d'une recommandation, comme le prévoyait d'ailleurs l'article 11 de la loi du 6 janvier 1978 alors en vigueur⁴.

Vous pourrez aisément écarter le moyen d'erreur de droit tiré de ce que la CNIL aurait appliqué à tort le régime des catégories particulières de données mentionnées à l'article 9 du RGPD, c'est-à-dire les données dites sensibles, qui exige en principe un consentement explicite, alors que le numéro de carte bancaire n'est pas au nombre de ces données. La délibération se borne à appliquer le régime de droit commun prévu à l'article 6, qui prévoit qu'un traitement est fondé sur le consentement ou sur une autre des bases légales énumérées.

La société soutient ensuite que la CNIL a méconnu le champ d'application de l'article 6 du RGPD en regardant le consentement comme une exigence cumulative des autres bases légales que cet article énumère. Mais ce n'est pas ce qu'elle a fait. Tout en écartant expressément la base légale prévue au b) du paragraphe 1 de l'article 6, à savoir le fondement contractuel, en-dehors des abonnements donnant lieu à paiements réguliers, elle a implicitement mais nécessairement exclu l'application des autres bases légales énumérées aux c) à f). Plus précisément, au titre du f) qui est l'enjeu central de ce litige, la CNIL a considéré que l'intérêt légitime d'une entreprise à conserver les données de carte bancaire en vue de faciliter la vie de ses clients en les dispensant de ressaisir leur numéro de carte bancaire pour procéder à un achat, c'est-à-dire à fluidifier le parcours client, ne prévalait pas sur les intérêts et les libertés et droits fondamentaux des clients, qui peuvent, de leur côté, légitimement ne pas souhaiter que l'opérateur conserve ces données en raison du mésusage qu'il pourrait en faire ou du risque qu'elles soient volées.

⁴ Etant précisé, naturellement, que les Etats membres ne sauraient ajouter de nouveaux cas de licéité ni prévoir des exigences supplémentaires qui viendraient modifier la portée de l'une des bases légales (V. déjà, sous l'empire de la directive 95/46 : CJUE, 24 novembre 2011, *ASNEF et FECEMD*, C-468/10 et C-469/10, pts. 30 et 32).

Dans la **balance des intérêts** que consacrent ces dispositions, il y a lieu, comme le recommandait le G29 dans son avis de 2014 sur la question, de tenir compte, d'un côté, de l'importance et de l'évidence de l'intérêt légitime du responsable de traitement et, de l'autre, de l'incidence du traitement sur les personnes concernées eu égard à la nature des données traitées, à la façon dont elles le sont, au statut du responsable de traitement et des personnes concernées et aux attentes raisonnables de ces dernières – ce dernier critère étant mis en exergue par le considérant 47 du RGPD⁵.

Il n'est pas contestable que les entreprises justifient d'un intérêt légitime à conserver les numéros de carte bancaire de leurs clients en vue de faciliter des paiements ultérieurs, notamment dans le cadre d'un dispositif de paiement en un clic. Ce faisant, elles poursuivent deux objectifs convergents : simplifier la vie des clients et, surtout, maximiser leur chiffre d'affaires. Elles contribuent ce faisant au développement de la consommation et à la croissance économique – même si les petits commerces de proximité ne sont sans doute pas du même avis⁶.

Mais on ne peut davantage nier que cette donnée à caractère personnel qu'est le numéro de carte bancaire présente une **sensibilité certaine**. Il ne se passe pas un mois ou, au moins, un trimestre, sans qu'une entreprise mondialement connue ne soit l'objet de cyberattaques ayant pour objet et, hélas, souvent pour effet de subtiliser les données bancaires conservées par l'opérateur en vue de leur revente sur le *dark web*. Tel a été le cas, en mai dernier, d'Easyjet ou encore, pour rester dans le secteur du transport aérien, de British Airways en 2018, qui lui a valu une très lourde amende de l'ICO, la CNIL britannique. Aucune entreprise n'est à l'abri d'une cyberattaque sophistiquée et, en la matière, le risque 0 n'existe pas. Nous ne sommes par ailleurs pas convaincu qu'il y ait plus à craindre de la pratique consistant à renseigner le numéro de carte bancaire à chaque transaction, comme le soutient la société. Outre les hypermnésiques qui n'ont pas besoin de sortir physiquement la carte du portefeuille, un utilisateur avisé prendra soin de ne le faire qu'à l'abri des regards indiscrets, pour reprendre une expression consacrée.

⁵ « (...) l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée ».

⁶ Si cette base légale ne s'attache pas, formellement, à l'existence de considérations d'intérêt général venant au soutien de l'intérêt du responsable de traitement (encore que sont aussi inclus les intérêts légitimes de « tiers »), il est évident que celles-ci viennent renforcer la légitimité de sa démarche et le « poids » de son intérêt (V. en ce sens l'avis du G29 sur l'application de cette disposition sous l'empire de la directive 95/46, p. 39).

Sans doute le numéro de carte bancaire ne suffit-il pas, en principe, pour procéder à un paiement en ligne. En premier lieu, il faut aussi disposer du mois d'expiration et du cryptogramme visuel, aussi appelé code CVV, à savoir les trois chiffres inscrits au dos de la carte. Si la première donnée est en général enregistrée en même temps que le numéro de la carte par le e-commerçant, ce dernier ne doit pas conserver la seconde puisqu'elle a pour objet de garantir que la transaction est effectuée par le porteur de la carte. L'article 4 de la délibération attaquée le rappelle. Le client doit renseigner ce code à chaque transaction, ce qui constitue une sécurité supplémentaire.

En second lieu, le paiement en ligne suppose, de plus en plus souvent, une authentification. La modalité la plus courante est le code temporaire envoyé par SMS, dans le cadre du dispositif dit « 3DSecure », plus sûr que la fourniture de la date de naissance⁷. Mais jusqu'à récemment, il s'agissait d'une simple faculté pour le e-commerçant. La directive dite DSP 2⁸ exige désormais une « authentification forte » pour les paiements en ligne, dite aussi « authentification multi-facteurs », consistant en au moins deux facteurs d'authentification⁹. Le dispositif de « Clé digitale » déjà utilisé par de nombreuses banques s'inscrit dans ce cadre. La mise en œuvre de cette obligation, entrée en vigueur le 14 septembre 2019¹⁰, fait d'ailleurs l'objet d'un aménagement. En tout état de cause, outre qu'elle n'a rien d'infaillible, cette authentification souffre elle-même de dérogations, notamment pour les transactions en ligne de faibles montants¹¹.

Il n'est donc pas contestable – et l'analyse d'impact sur la vie privée du traitement « paiement flash » réalisé par la société l'admet elle-même¹², **que le vol du numéro de carte bancaire peut avoir des incidences très fâcheuses pour les clients**, sans même évoquer les frais liés à l'opposition¹³ et les désagréments de toutes natures qui résultent de l'indisponibilité de la carte et des démarches nécessaires pour la remplacer¹⁴.

⁷ Selon le rapport 2018 de l'Observatoire de la sécurité des moyens de paiement, le taux de fraude par paiement authentifiés est de 0,07 %, contre 0,21 % pour les transactions non authentifiées.

⁸ Directive (UE) 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (article 97).

⁹ Qui peuvent être basés sur la connaissance (d'un mot de passe, de la réponse à une question secrète...), sur la possession (un objet que seul l'utilisateur possède, comme son smartphone personnel) ou sur la biométrie.

¹⁰ Soit, conformément à l'article 115 de la directive, 18 mois après l'entrée en vigueur du règlement délégué (UE) 2018/389 de la Commission du 27 novembre 2017 complétant la directive par des normes techniques de réglementation relatives à l'authentification forte du client.

¹¹ Selon l'article 16 du règlement délégué, l'authentification forte peut ne pas être exigée pour les transactions d'un montant inférieur à 30 euros, à condition que, depuis la dernière authentification forte, il n'y ait pas eu plus de 5 opérations en ligne consécutives et que le montant cumulé des paiements n'excède pas 100 euros.

¹² Elle cote la gravité du risque de fuite de cette donnée au niveau « important » et admet elle-même que « l'accès illégitime [à ces données] pourrait être particulièrement impactant pour les droits et libertés des personnes concernées »

Notre conviction est que l'arbitrage entre l'expérience utilisateur et la protection de la donnée appartient non à l'entreprise, mais au détenteur de la carte bancaire. Et ce dernier doit en principe être mis en mesure de l'opérer préalablement et expressément, par un mécanisme d'*opt-in*, sur la base d'une information complète sur les tenants et aboutissants d'un tel choix, et non simplement *a posteriori* par un droit d'opposition qu'il peut négliger d'exercer. L'entreprise n'a pas à se substituer au client, dans une logique presque paternaliste, pour définir ce qui est bon pour ce dernier. Certains, dont nous sommes, trouveront très pratique de ne pas avoir à saisir leur numéro de carte ; d'autres, qui sont probablement majoritaires, estimeront plus importants de préserver la confidentialité de leurs données bancaires. Le nombre de plaintes adressées chaque année à la CNIL sur ce thème – 142 en 2018 – confirment la forte sensibilité des internautes à cette problématique.

La circonstance mise en avant par CDiscount qu'une immense majorité des internautes réalisent plusieurs dizaines d'achats en ligne par an est inopérante. Cette information ne préjuge pas de la récurrence de leurs achats sur un même site, donc de la probabilité que le même internaute procède à un paiement sur ce site à brève échéance. L'idée qu'elle suggère de permettre l'*opt-out* à partir d'une certaine fréquence d'achats sur l'année serait quant à elle source d'une grande insécurité juridique¹⁵. La soupape imaginée par la CNIL, fondée sur l'existence manifeste d'une relation commerciale régulière attestée, à tout le moins, par la souscription d'une option facilitant les transactions ultérieures, est plus convaincante.

Nous pensons donc que la CNIL n'a pas méconnu le RGPD en estimant que le consentement de la personne devait par principe être recueilli en cas d'achats ponctuels¹⁶.

¹³ L'opposition est une obligation (art. L. 133-17 CMF).

¹⁴ On peut noter que la sensibilité de ces données a justifié que le paragraphe 2 de l'article 94 de cette directive DSP2, transposé à l'article L. 521-5 du code monétaire et financier, pose un principe de consentement, selon lequel les prestataires de services de paiement n'ont accès, ne traitent et ne conservent les données à caractère personnel nécessaires à l'exécution des services qu'avec le **consentement exprès de l'utilisateur**, sous le contrôle de la CNIL (art. L. 521-7 CMF). Si le CEPD lui-même a estimé que ce consentement n'avait pas la même portée que le consentement régi par le RGPD (V. la lettre du 5 juillet 2018 adressé par le CEPD à la députée Sophie in 't Veld, EDPB-84-2018), et si ce texte n'est pas applicable aux e-commerçants eux-mêmes, il témoigne tout de même de l'extrême vigilance du législateur européen sur le traitement de ces données.

¹⁵ A cet égard, la position exprimée par CDiscount dans un courrier du 15 juin 2018, qui se limitait à examiner la probabilité qu'un client effectue une nouvelle commande sur son site dans les douze mois d'un achat, ne serait certainement pas suffisante.

¹⁶ Même si ce point est hors débat, précisons que nous ne voyons rien, dans la situation de CDiscount, qui justifierait qu'elle échappe à cette exigence. Elle opère un traitement massif, qui s'adresse à des catégories très diverses d'internautes dont certains peuvent être vulnérables, sa position de marché lui permet plus aisément

Il est reproché à la Commission d'avoir **raisonné abstraitement**, sans tenir compte de la diversité des situations et des responsables de traitement, dont certains, comme CDiscount, offrirait des garanties permettant de faire pencher la balance des intérêts en leur faveur. Même si la société ne s'en prévaut pas, il est vrai que la Cour de justice a jugé que les dispositions équivalentes de la directive 95/46, ancêtre du RGPD, s'opposent à ce qu'un État membre exclue de façon catégorique et généralisée la possibilité pour certaines catégories de données à caractère personnel d'être traitées au titre de l'intérêt légitime, sans permettre une pondération des droits et des intérêts opposés en cause dans un cas particulier. Un État membre ne saurait ainsi prescrire, pour ces catégories, de manière définitive, le résultat de la pondération des droits et des intérêts opposés, sans permettre un résultat différent en raison de circonstances particulières d'un cas concret (CJUE, 19 octobre 2016, *Breyer*, C-582/14, pt. 62¹⁷)

Mais cette jurisprudence ne nous paraît pas faire obstacle à ce que soient identifiés des « scénarios-types » précis dans lesquels cette base légale ne peut pas jouer car la balance des intérêts sera par principe défavorable au responsable de traitement, compte tenu non seulement de la nature des données, mais aussi de celle du traitement, notamment ses finalités, et les intérêts des personnes en jeu. On peut d'autant moins faire le reproche à la CNIL d'avoir adopté une approche fruste que, comme on l'a dit, elle a distingué, de manière au contraire assez fine, les différentes configurations relationnelles entre le client et le site de e-commerce et admis la base légale de l'intérêt légitime en présence d'une « relation commerciale régulière ». Vous n'êtes clairement pas ici face à une interdiction générale et absolue comme celle des *cookie walls* que vous avez récemment sanctionnée et dont la société se prévaut¹⁸. En tout état de cause, à l'instar de lignes directrices, s'il s'avérait que, dans un cas particulier qui n'a pas été envisagé, la balance des intérêts devait pencher en faveur de l'entreprise, la CNIL serait tenue de l'admettre¹⁹. Signalons au passage que les spécificités

d'imposer ses vues aux clients qu'un petit e-commerçant, et les données bancaires sont transmises et traitées par des sous-traitants, dont son AIPD indique qu'ils constituent le point de vulnérabilité. Les mesures de sécurisation dont elle fait état (pour l'essentiel, elle indique qu'en cas de changement d'adresse du client, ce dernier doit de nouveau saisir son numéro de carte bancaire) ne nous paraissent pas changer la donne.

¹⁷ CJUE, 24 novembre 2011, *ASNEF et FECEMD*, C-468/10 et C-469/10, pts. 30 et 32.

¹⁸ CE, 19 juin 2020, *Association des agences-conseils en communication et autres*, n° 434684, aux T.

¹⁹ Dans son avis sur ces dispositions (avis 06/2014 du 9 avril 2014, WP 217), alors prévues par la directive 95/46, le G29 préconisait une approche en deux temps : une analyse préliminaire fondée sur la nature des données, la façon dont elles sont traitées, les attentes raisonnables des personnes concernées et le statut du responsable de traitement et de la personne concernée ; et, si cette analyse liminaire ne permet pas de trancher, la prise en compte des mesures prises et garanties apportées par le responsable de traitement à titre complémentaire, qui peut éventuellement faire pencher la balance en sa faveur (pp. 45-47).

dont se prévaut CDiscount devant vous ne nous paraissent pas de nature à justifier qu'il soit dérogé à cette règle pour ce qui la concerne.

La société ne peut, ensuite, utilement soutenir qu'il résulterait de la délibération une atteinte excessive à la **liberté d'entreprendre** dès l'instant qu'elle fait une exacte application du RGPD et que ce règlement n'est pas argué de contrariété au droit primaire. En tout état de cause, il n'y a potentiellement, entre l'*opt-in* et l'*opt-out*, que l'espace d'une case précochée ou non, et si les conséquences économiques ne sont sans doute pas négligeables, l'atteinte portée à la liberté d'entreprendre n'est pas disproportionnée au regard du motif d'intérêt général qui la justifie.

Reste le moyen tiré de la **rupture d'égalité** entre les acteurs du e-commerce français soumis à cette recommandation, parce que relevant du champ de compétence territoriale de la CNIL, et les autres. Concrètement, CDiscount cible ici Amazon EU, situé au Luxembourg, qui détient Amazon France et dont il semble acquis pour elle qu'elle relève à titre principal de l'autorité de contrôle luxembourgeoise. De fait, nous constatons qu'Amazon a retenu une autre formule, dont la légalité interroge au regard de l'exigence d'un consentement libre et éclairé, qui consiste à obliger le client à enregistrer sa carte bancaire s'il souhaite procéder à un paiement en ligne au comptant.

Ce moyen est à nos yeux inopérant dans le présent litige. Les distorsions de concurrence que dénonce CDiscount sont la résultante des règles de compétence territoriale des autorités de contrôle et de la doctrine adoptée par chacune d'elles. La CNIL ne peut, par construction, prétendre élaborer une recommandation applicable à des acteurs qui ne relèvent pas de sa compétence. La solution alternative reviendrait donc à lui interdire de prendre une position interprétative susceptible d'introduire des distorsions de concurrence au sein de l'Union, au bénéfice ou au détriment des entreprises soumises à son contrôle, compte tenu de la doctrine de ses homologues. Concrètement, il lui faudrait attendre soit qu'une position commune ait été adoptée dans le cadre du mécanisme de contrôle de la cohérence, c'est-à-dire via une décision contraignante du comité européen de la protection des données ou, à la limite, via des lignes directrices de ce dernier quoiqu'elles n'aient pas de force obligatoire ; soit que la Cour de justice de l'Union européenne ait fixé la jurisprudence pour l'ensemble de l'Union. Il appartient au contraire à la CNIL d'exercer pleinement sa compétence, qu'elle tire tant du RGPD que de la loi du 6 janvier 1978, d'édicter des lignes directrices et recommandations afin d'éclairer les acteurs du secteur sur sa doctrine de mise en œuvre de la réglementation.

Précisons tout de même que le champ de compétence territoriale de la CNIL est large puisqu'il recouvre tous les responsables de traitement disposant d'un établissement en France dans le

cadre duquel les données sont traitées. Tel est le cas d'Amazon France. La recommandation s'applique donc à cet établissement. Toutefois, en cas de litige concernant ce traitement transfrontalier, s'il est avéré qu'Amazon dispose d'un établissement principal au Luxembourg, la Commission nationale pour la protection des données de ce pays serait l'autorité chef de file et la CNIL serait seulement « autorité de contrôle concernée ». A ce dernier titre, elle pourrait, si elle estimait la pratique d'Amazon contraire à sa recommandation et si la CNPD luxembourgeoise était a priori d'un avis inverse, émettre une « objection pertinente et motivée » assise sur sa doctrine propre, pour provoquer une saisine du CEPD.

Vous pourriez seulement, à notre avis, admettre l'opérance d'un moyen tiré de l'erreur manifeste d'appréciation à avoir élaboré une doctrine en décalage avec le reste de l'Union européenne – étant rappelé que vous exercez un contrôle restreint sur l'opportunité, pour une autorité de régulation, de publier une prise de position à l'intention des acteurs du secteur (CE, Ass., 21 mars 2016, *Sté Fairvesta Internal Gmbh et autres*, n° 368082-368083-368084, au Rec.). Mais à supposer qu'on extirpe un tel moyen des écritures qui vous sont présentées, nous ne sommes pas convaincu de son bien-fondé.

La sensibilité du sujet, exacerbée par l'initiative prise par CDiscount, justifiait que la CNIL intervienne. Il n'est absolument pas démontré qu'elle serait isolée au sein de l'Union européenne et que sa doctrine pénaliserait gravement les sociétés opérant essentiellement en France. La CNIL a en outre, parallèlement, porté l'inscription de ce sujet au programme de travail du CEPD. Enfin, nous rappellerons à la société qu'il lui est loisible de saisir la **Commission européenne**, gardienne du respect du RGPD, afin qu'elle suscite une position harmonisée au niveau de l'Union via une saisine formelle du CEPD, voire qu'elle ouvre une procédure d'infraction contre un Etat membre abritant une autorité de contrôle chef de file un peu trop laxiste à ses yeux.

PCMNC au rejet de la requête.