

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Les modalités de recueil du consentement en matière de cookies non essentiels : la chasse aux pratiques non conformes menée par la CNIL se poursuit

Gobert, Alix

Published in:

Revue du Droit des Technologies de l'information

Publication date:

2023

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Gobert, A 2023, 'Les modalités de recueil du consentement en matière de cookies non essentiels : la chasse aux pratiques non conformes menée par la CNIL se poursuit: observations sous Commission nationale de l'informatique et des libertés (CNIL), décision du 29 décembre 2022', *Revue du Droit des Technologies de l'information*, numéro 88-89, pp. 135-158.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

OBSERVATIONS¹

Les modalités de recueil du consentement en matière de cookies non essentiels : la chasse aux pratiques non conformes menée par la CNIL se poursuit

I. INTRODUCTION

Quiconque consulte un site web est désormais habitué de commencer sa visite en étant confronté à une « bannière de cookies » surgissant sur son écran dès l'ouverture de la page web et lui enjoignant de se positionner quant au placement de cookies sur le terminal utilisé.

Ces bannières de cookies – souvent considérées comme envahissantes et gênantes pour le confort de navigation – répondent à une obligation légale prévue par directive (CE) 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques² (ci-après : « directive ePrivacy »), qui impose aux acteurs du web d'obtenir le consentement des utilisateurs préalablement au dépôt et à l'inscription des cookies non

essentiels³ dans les terminaux utilisés pour la navigation⁴.

Depuis plusieurs années, afin de concilier leurs propres intérêts économiques avec la réglementation européenne, les acteurs du web ont fait preuve d'énormément de créativité afin de développer des bannières de cookies qui, en apparence, semblent respecter l'exigence du consentement préalable⁵.

La décision rendue par la Commission nationale de l'informatique et des libertés⁶ (ci-après : « CNIL ») à l'encontre du réseau social TikTok en

³ Les cookies sont de petits fichiers texte qui peuvent être déposés sur l'ordinateur des utilisateurs lorsqu'ils visitent des sites web. Ces fichiers contiennent différentes informations sur les utilisateurs. Une distinction doit être réalisée entre les cookies dit « essentiels » et les cookies dit « non essentiels ». Les cookies « essentiels » ne sont pas soumis au consentement et sont ceux qui ont pour finalité exclusive de permettre ou de faciliter une communication par voie électronique ou qui sont strictement nécessaires à la fourniture d'un service de communication en ligne (la CNIL cite, à titre d'exemple, les cookies conservant le choix exprimé par les utilisateurs quant au dépôt des traceurs ou encore les traceurs de personnalisation de l'interface utilisateur, par exemple quant au choix de la langue). À l'inverse, les cookies « non essentiels » regroupent tous les cookies qui ne sont pas essentiels au bon fonctionnement du site web (la CNIL cite, à titre d'exemple, les cookies liés aux opérations relatives à la publicité ciblée). Ces cookies sont soumis à l'obligation du recueil d'un consentement préalable prévue à l'article 5, § 3, de la directive ePrivacy.

⁴ Article 5, § 3, de la directive « ePrivacy ».

⁵ *Idem*.

⁶ La Commission nationale de l'informatique et des libertés est l'autorité de protection des données française instituée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après : « CNIL »).

¹ Alix Gobert, chercheuse au Nadi/CRIDS de l'Université de Namur.

² Directive (CE) 2002/58 du Parlement européen et du Conseil 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 (directive vie privée et communications électroniques), *J.O.*, L 201, 31 juillet 2002, telle que modifiée par la directive (CE) 2009/136 du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive (CE) 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *J.O.*, L 337/11, 18 décembre 2009.

date du 29 décembre 2022⁷ s'attaque principalement au *design* de la bannière de cookies ainsi qu'aux modalités de recueil du consentement au dépôt de cookies⁸.

Dans le cadre de cette observation, nous dresserons dans un premier temps le contexte général de lequel la CNIL a commencé à investiguer auprès des acteurs du web en matière de cookies. Ensuite, nous analyserons la question de la compétence matérielle de la CNIL ainsi que les manquements aux obligations en matière de dépôt et d'écriture de cookies qui ont été identifiés par la CNIL. À cette occasion, nous ferons le point sur les obligations en matière de consentement et d'information pesant sur les acteurs du web lorsqu'ils recourent à des cookies dans le cadre de leurs activités. Enfin, dans un dernier temps, nous ouvrirons la réflexion quant à une reconnaissance croissante du principe d'autonomie individuelle au sein du droit positif européen.

II. CONTEXTE GÉNÉRAL

Au niveau européen, le cadre légal applicable aux cookies demeure complexe, en raison, notamment, de la pluralité de textes applicables. Il s'agit principalement du règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre

circulation de ces données⁹ (ci-après «RGPD») et de la directive ePrivacy¹⁰.

Alors qu'une simplification du régime légal applicable aux cookies est attendue depuis 2018 avec une éventuelle adoption du règlement européen ePrivacy qui devrait abroger et remplacer la directive du même nom, celui-ci est toujours en cours de négociation au Parlement européen et tarde à être adopté¹¹.

Dans l'attente de ce règlement, la CNIL a entamé, depuis 2019, un travail d'envergure destiné, d'une part, à interpréter et à clarifier les règles applicables en matière de dépôt de cookies et, d'autre part, à accompagner les acteurs du web dans leur implémentation des exigences légales¹². Dans ce cadre, elle avait annoncé, en 2019, la mise en œuvre d'une stratégie globale de mise en conformité, à travers un plan d'action découpé en deux grandes étapes: l'adoption de nouvelles lignes directrices en juillet 2019 destinées à clarifier, synthétiser et interpréter la réglementation applicable¹³, et l'émission de

⁹ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.*, L 119, 4 mai 2016.

¹⁰ A. DELFORGE, «Le placement des cookies sur un site web: enfin la fin de la récréation ou le début de la fin?», *R.D.T.I.*, 87/2022, p. 127.

¹¹ Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), COM/2017/010 final (ci-après «Proposition ePrivacy»).

¹² «Ciblage publicitaire en ligne: quel plan d'action de la CNIL?», consulté le 13 février 2023, disponible sur: www.cnil.fr; «Cookies et autres traceurs: la CNIL publie de nouvelles lignes directrices», consulté le 13 février 2023, disponible sur: www.cnil.fr.

¹³ Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un

⁷ Délibération de la formation restreinte n° SAN-2022-027 du 29 décembre 2022 concernant les sociétés TikTok Information Technologies UK et TikTok Technology Limited, disponible en intégralité sur: https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046977994?init=true&page=1&query=SAN-2022-027&searchField=ALL&tab_selection=all (ci-après: «Décision TikTok»).

⁸ Notons que la décision concerne uniquement le site web www.tiktok.com et non pas l'application mobile.

recommandations pratiques à destination des acteurs du web sommés de recueillir un consentement valable des utilisateurs pour l'inscription de cookies¹⁴. À l'issue de l'adoption de cette recommandation, une période transitoire de six mois avait été laissée aux acteurs pour s'y conformer. Elle a pris fin le 1^{er} avril 2021¹⁵.

Depuis cette date et comme elle l'avait annoncé, la CNIL a entamé ses investigations et envoie aux différents acteurs du web récalcitrants des mises en demeure leur enjoignant de mettre leur site internet en conformité. Est en cause, notamment, la pratique des *dark patterns*¹⁶, c'est-à-dire le recours à des modalités de recueil du consentement qui sont configurées de telle sorte qu'elles influencent le comportement des utilisateurs en faveur de l'octroi de leur consentement.

À l'issue de ces enquêtes, plusieurs décisions ont été adoptées par la commission restreinte de la CNIL en vue de sanctionner certains

acteurs¹⁷. La décision à l'origine de la présente observation fait partie d'une salve de sanctions par lesquelles la CNIL punit des acteurs désobéissants. Ces décisions sont fondamentales, non seulement parce qu'elles donnent corps aux lignes directrices et à la recommandation de la CNIL, mais également parce qu'elles s'inscrivent dans une problématique qui dépasse l'autorité de protection des données française et dont les enseignements permettent d'éclairer et d'inspirer les autres autorités de protection des données nationales sur les exigences à avoir en matière de consentement.

Notons que si la CNIL a fait de la réglementation sur les cookies son cheval de bataille, cette tendance se retrouve également auprès d'autres autorités nationales, notamment au sein de l'Autorité de protection des données belge qui a enquêté dernièrement auprès de nombreux sites web¹⁸ et a annoncé faire des cookies l'une de ses priorités de l'année 2023, notamment en s'attelant à l'adoption d'une recommandation destinée à clarifier sa position concernant la réglementation applicable¹⁹.

Parallèlement au travail de fond mené par certaines autorités de protection des données

utilisateur (notamment aux cookies et autres traceurs). Ces lignes directrices ont depuis lors été abrogées et remplacées par la délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux «cookies et autres traceurs») et abrogeant la délibération n° 2019-093 du 4 juillet 2019 (ci-après : «Lignes directrices de la CNIL du 17 septembre 2020»).

¹⁴ Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux «cookies et autres traceurs» (ci-après : «Recommandation de la CNIL du 17 septembre 2020»).

¹⁵ Décision «TikTok», point 98.

¹⁶ Voy. EDPB, «Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them», 21 mars 2022, p. 2, qui définit les dark patterns comme étant «des interfaces et des expériences utilisateur mises en œuvre sur les plateformes de médias sociaux qui conduisent les utilisateurs à prendre des décisions potentiellement préjudiciables concernant le traitement de leurs données à caractère personnel» (traduction libre).

¹⁷ Voy. notamment : délibération de la formation restreinte n° SAN-2022-023 du 19 décembre 2022 concernant la société Microsoft Ireland Operations Limited»; délibération de la formation restreinte n° SAN-2021-024 du 31 décembre 2021 concernant la société Facebook Ireland Limited; délibération de la formation restreinte n° SAN-2022-026 du 29 décembre 2022 concernant la société VOOODO.

¹⁸ Voy. notamment : décision n° 85/2022 du 25 mai 2022; décision n° 103/2022 du 16 juin 2022. L'APD a également mené plusieurs enquêtes concernant les cookies auprès de médias belges qui ont abouties à des transactions avec les acteurs concernés : voy. notamment : décision n° 168/2022 du 22 novembre 2022; décision n° 157/2022 du 4 novembre 2022; décision n° 151/2022 du 21 octobre 2022; décision n° 150/2022 du 21 octobre 2022.

¹⁹ «L'APD définit ses priorités pour l'année 2023», consulté le 9 février 2023, disponible sur : www.autoriteprotectiondonnees.be/citoyen/lapd-definit-ses-priorites-pour-lannee-2023.

nationales, le Comité européen de la protection des données²⁰ (ci-après «CEPD») – sous l'impulsion des 500 plaintes introduites par le collectif NOYB²¹ auprès de 18 autorités de protection des données concernant le *design* de bannières de cookies – avait mis en place, en 2021, un groupe de travail rassemblant plusieurs autorités de protection des données. Son objectif était de dégager une vision commune afin de coordonner les réponses à apporter à ces plaintes²². Cela a abouti à l'adoption d'un rapport qui a été publié le 17 janvier 2023 – soit moins d'un mois après l'adoption de la décision commentée – reprenant différents exemples de pratiques considérées comme non conformes en matière de recueil du consentement au dépôt de cookies²³.

III. LA COMPÉTENCE MATÉRIELLE DE LA CNIL : EXCLUSION DÉFINITIVE DU MÉCANISME DU « GUICHET UNIQUE »

Alors que la question de l'application du mécanisme du « guichet unique » à la problématique du dépôt et de l'écriture de cookies a déjà fait

couler beaucoup d'encre, on peut l'estimer aujourd'hui définitivement tranchée²⁴.

Le mécanisme du « guichet unique » est prévu à l'article 56 du RGPD²⁵ qui dispose qu'en cas de traitement transfrontalier de données à caractère personnel, l'autorité de contrôle compétente pour agir en tant que chef de file est celle de l'établissement principal ou de l'établissement unique du responsable du traitement. La société TikTok ayant son établissement principal en Irlande, l'application du mécanisme du guichet unique aboutirait à la désignation de l'Autorité de protection des données irlandaise comme autorité compétente pour connaître de l'affaire, privant la CNIL française de toute compétence.

Dans la lignée de ses précédentes décisions, telles que celles rendues à l'encontre de Microsoft et de Google²⁶, la CNIL écarte l'application du mécanisme du guichet unique et se déclare matériellement compétente pour contrôler et sanctionner les opérations d'accès ou d'ins-

²⁰ Le Comité européen de la protection des données («European Data Protection Board»), est un organe de l'Union institué par l'article 68 du RGPD et qui a notamment pour mission de surveiller et de garantir la bonne application du RGPD ainsi que d'encourager la coopération entre autorités de l'UE chargées de la protection des données.

²¹ NOYB («None of your business») est une organisation à but non lucratif créée par Max Schrems dont l'objet est la protection de la vie privée et dont le champ d'action s'étend à toute l'Europe. Elle vise principalement à mettre fin aux violations de la vie privée dans le secteur privé et à faire respecter le RGPD.

²² «EDPB determines privacy recommendations for use of cloud services by public sector & adopts report on Cookie Banner Task Force», consulté le 10 février 2023, disponible sur : https://edpb.europa.eu/news/news/2023/edpb-determines-privacy-recommendations-use-cloud-services-public-sector-adopts_en.

²³ EDPB, «Report of the work undertaken by the Cookie Banner Taskforce EDPB», 17 janvier 2023, disponible sur : https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf.

²⁴ La problématique du « guichet unique » a en effet été discutée dans plusieurs décisions de la CNIL portant sur la problématique de l'écriture et du dépôt de cookies. Voy. notamment : délibération de la formation restreinte n° SAN-2022-023 du 19 décembre 2022 concernant la société Microsoft Ireland Operations Limited ; délibération de la formation restreinte n° SAN-2021-024 du 31 décembre 2021 concernant la société Facebook Ireland Limited ; délibération de la formation restreinte n° SAN-2021-023 du 31 décembre 2021 concernant les sociétés Google LLC et Google Ireland Limited ; délibération de la formation restreinte n° SAN-2022-025 du 29 décembre 2022 concernant la société Apple Distribution International.

²⁵ Article 56.1 RGPD : « Sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60 ».

²⁶ Délibération n° SAN-2022-023 du 19 décembre 2022, points 22-28 ; délibération n° SAN-2021-023 du 31 décembre 2021, points 57 et 58.

cription d'informations dans les terminaux des utilisateurs du réseau social TikTok France²⁷.

La position de la CNIL peut être résumée comme suit : les traitements des données à caractère personnel obtenues à la suite du dépôt de cookies sur les terminaux des utilisateurs d'un site internet constituent des activités de traitements soumises au RGPD²⁸. De surcroît, les opérations de dépôt et d'inscription d'informations sous la forme de cookies sur les terminaux des utilisateurs constituent une fourniture de services de communications électroniques, lesquels sont spécifiquement réglementés par la directive ePrivacy²⁹. L'article 15*bis* de cette directive régit spécifiquement la question de la mise en œuvre et du contrôle des obligations qu'elle comporte en prévoyant notamment qu'en matière de fourniture de services de communications électroniques, chaque État membre doit désigner, dans sa législation nationale, une autorité chargée de contrôler le respect des dispositions de la directive et, le cas échéant, de sanctionner les opérateurs qui en enfreindraient les règles. Notons que, en France, la CNIL a été désignée par les articles 16 et 20 de la loi Informatique et Libertés³⁰ comme autorité compétente pour contrôler et, le cas échéant, sanctionner le non-respect des dispositions de cette directive. Les règles spéciales dérogeant

aux règles générales, dans la mesure où la directive ePrivacy régit spécifiquement la question de sa mise en œuvre et de son contrôle au sein de son article 15*bis* et que cette réglementation ne renvoie aucunement au mécanisme du « guichet unique » prévu par le RGPD, il n'y a pas lieu d'en faire application.

Cette position a par ailleurs été validée par le Conseil d'État français dans deux décisions rendues à la suite de recours introduits par Google et Amazon³¹. Ces derniers contestaient la compétence de la CNIL quant aux sanctions prononcées à leur égard en matière de dépôt et d'écriture de cookies. Cette position est également suivie par le CEPD qui a indiqué que lorsque le litige concerne le placement de cookies, la réglementation applicable est bien la législation nationale transposant la directive ePrivacy³².

Notons que l'adoption du règlement ePrivacy ne devrait pas venir bousculer cette position. En effet, alors que dans sa première mouture, le texte prévoyait un renvoi aux chapitres VI et VII du RGPD pour le contrôle de ses dispositions³³ – soit, notamment, à l'application du mécanisme du guichet unique – en invoquant « les fortes synergies entre les questions générales de protection des données et la confidentialité des communications »³⁴, la dernière

²⁷ Décision « TikTok », points 29 et 32.

²⁸ Le « traitement » est défini par l'article 4, 2), du RGPD comme étant : « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

²⁹ Décision « TikTok », points 25 et 26.

³⁰ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

³¹ Conseil d'État (France), décision n° 451423, lecture du 27 juin 2022, point 8 ; Conseil d'État (France), décision n° 449209, lecture du 28 janvier 2022, point 12.

³² EDPB, « Report of the work undertaken by the Cookie Banner Taskforce », 17 janvier 2023, p. 4.

³³ L'article 18 de la version initiale de la proposition de règlement ePrivacy (version du 10 janvier 2017) prévoyait que : « L'autorité ou les autorités de contrôle indépendantes chargées du contrôle de l'application du règlement (UE) 2016/679 sont également chargées du contrôle de l'application du présent règlement. Les chapitres VI et VII du règlement (UE) 2016/679 s'appliquent par analogie (...) ».

³⁴ Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la

version de la proposition a supprimé ce renvoi aux dispositions générales du RGPD pour en revenir au mécanisme de contrôle tel qu'il existe aujourd'hui à l'article 15*bis* de la directive ePrivacy³⁵.

IV. LES MANQUEMENTS AUX OBLIGATIONS EN MATIÈRE DE DÉPÔT ET D'ÉCRITURE DE COOKIES

A. Considérations générales

La question de la compétence matérielle de la CNIL concernant le dépôt de cookies a mis en évidence la difficile juxtaposition de textes législatifs européens. En l'espèce, il s'agit de jongler avec, d'une part, le RGPD qui s'applique de manière générale aux traitements de données à caractère personnel et, d'autre part, avec la directive ePrivacy qui s'applique spécifiquement aux opérations d'écriture et de dépôt de cookies en ce qu'ils sont constitutifs de services de communications électroniques. Alors qu'en matière de compétence, le conflit de loi se résout par l'application de la réglementation spécifique au détriment de la réglementation générale, en ce qui concerne la question du consentement, les deux textes législatifs sont appelés à collaborer. En effet, la directive ePrivacy prévoit explicitement en son article 2, f) que « le "consentement" d'un utilisateur ou d'un abonné à un service de communication électronique correspond au "consentement" de la personne concernée figurant dans la directive 95/46/CE »³⁶. Pour être valable, le consentement au dépôt de cookies non essentiels doit donc correspondre, par analogie, aux critères établis par le RGPD, soit à une manifestation de volonté libre, spécifique, éclairée et

univoque et prendre la forme d'un acte positif clair³⁷.

S'il est donc indiscutable que le consentement au dépôt de cookies doit être analysé au regard des critères établis par le RGPD, la forme qu'il doit revêtir pour répondre à ces différents critères est moins claire. L'investigation menée par la CNIL sur le site web de la société chinoise et l'analyse qu'elle produit dans sa décision ont été l'occasion, pour elle, premièrement, d'interpréter la notion de consentement libre et éclairé et, deuxièmement, d'appliquer et d'affiner les critères qu'elle avait présentés au préalable dans ses lignes directrices et dans sa recommandation.

B. Le caractère libre du consentement

Lors de son contrôle en ligne, la rapporteuse a constaté que lorsque l'on arrivait sur le site web de TikTok, alors que la bannière de cookies affichait un bouton « Tout accepter », aucun bouton équivalent permettait de refuser, en un seul clic, le dépôt des cookies. Après investigation, il ressort que pour refuser explicitement les cookies, l'utilisateur devait d'abord cliquer sur le bouton « Gérer les paramètres » qui se trouvait au même niveau que le bouton « Tout accepter », pour ensuite devoir cliquer sur « Ouvrir les paramètres de cookies » – où apparaissait l'interface permettant à l'utilisateur d'accepter et/ou de refuser chaque cookie séparément – et enfin, valider son choix en cliquant sur « Enregistrer »³⁸. Autrement dit, alors qu'un seul clic permettait aux utilisateurs d'accepter le dépôt des cookies, pas moins de trois clics étaient nécessaires pour permettre

directive 2002/58/CE, Exposé des motifs, p. 11 (version initiale du 10 janvier 2017).

³⁵ Proposition ePrivacy, article 18, dernière version du 10 février 2021, n° 6087/21.

³⁶ La directive 95/46/CE a été abrogée et remplacée depuis lors par le RGPD.

³⁷ Article 4, 11), du RGPD définissant le « consentement de la personne concernée » comme étant : « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

³⁸ Décision « TikTok », point 67.

aux plus opiniâtres de refuser le dépôt de ces mêmes cookies.

Le caractère libre est l'une des pierres angulaires du consentement. Le RGPD lui a d'ailleurs consacré un considérant spécifique qui précise que «le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix»³⁹ ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice»⁴⁰. Il est désormais communément admis que le caractère libre du consentement au dépôt de cookies est incompatible avec une quelconque forme de pression à l'égard des internautes⁴¹. En effet, un utilisateur qui ne consent pas au dépôt de cookies ne peut pas être préjudicié pour cette seule raison – par exemple en se voyant refuser l'accès au site web concerné – et doit pouvoir bénéficier d'une alternative lui permettant de profiter des mêmes services qu'un autre utilisateur qui y aurait consenti⁴². On a alors vu fleurir des bannières de cookies semblables à celle mise en place sur le site web de TikTok qui – si elles permettent effectivement à l'utilisateur de consentir ou de refuser les cookies sans en être préjudicié – sont néanmoins pensées et configurées de telle sorte qu'elles rendent l'acceptation des cookies beaucoup plus attractive et bien plus simple que le refus⁴³.

Face à ce constat, la CNIL rappelle qu'elle a, dans ses lignes directrices⁴⁴ ainsi que dans sa recommandation⁴⁵, insisté sur le fait que pour que le consentement tel qu'il est requis à l'article 82 de la loi Informatique et Liberté⁴⁶ – qui transpose en droit français la directive ePrivacy – soit valable, l'utilisateur doit bénéficier d'une véritable liberté de choix. Ceci implique qu'il doit être aussi aisé d'accepter les cookies que de les refuser et que les modalités mises en œuvre par les organismes afin d'obtenir le consentement des utilisateurs ne doivent pas être pensées et configurées en vue de favoriser, de quelque manière que ce soit, l'obtention du consentement⁴⁷. La CNIL insiste sur le fait que si consentir au dépôt des cookies est plus aisé que d'y renoncer, il existe un risque réel qu'une grande partie des utilisateurs donnent leur consentement uniquement parce que la démarche d'acceptation est bien plus simple et accessible, auquel cas le consentement ne remplit pas les conditions de qualité et de validité requises.

Une fois sa position concernant son interprétation du caractère libre du consentement rappelée, la CNIL procède ensuite à une analyse *in concreto* des modalités de recueil du consentement mises en place par le site web www.tiktok.com.

³⁹ Nous soulignons.

⁴⁰ Considérant 42 du RGPD.

⁴¹ A. DELFORGE, «Le placement de "cookies" sur un site web: la Cour de justice fait le point, l'APD commence à sanctionner», *R.D.T.I.*, 78/2020, p. 109.

⁴² EDPB, «Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679», 4 mai 2020, p. 8; A. MICHEL, «Le traçage comportemental des internautes sur les réseaux sociaux: l'affaire des "cookies Facebook", véritable saga judiciaire?», *Observations sous Civ. Bruxelles* (24^e ch. N), 16 février 2018, 2016/153/A, *R.D.T.I.*, 74/2019, p. 88; lignes directrices de la CNIL du 17 septembre 2020, *op. cit.*, point 17.

⁴³ P.-O. PIELAET, «La privacy by design à l'épreuve des "dark patterns"», *R.D.T.I.*, 80/2020, p. 40.

⁴⁴ Lignes directrices de la CNIL du 17 septembre 2020, *op. cit.*

⁴⁵ Recommandation de la CNIL du 17 septembre 2020, *op. cit.*

⁴⁶ Article 82 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés: «(...). Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son consentement qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle».

⁴⁷ Décision «TikTok», point 66.

C. Vers des conditions particulières liées à la forme du refus

Pour sa défense, TikTok arguait que, bien que le bouton «Tout accepter» ne trouve pas son antonyme direct sur la bannière de cookies, il n'en reste pas moins que l'utilisateur continuant sa visite du site web sans poser d'action était considéré comme ayant implicitement refusé les cookies et que dès lors, aucun cookie non essentiel n'était installé sur son terminal⁴⁸. Il était donc, selon la société chinoise, aussi aisé de refuser les cookies que de les accepter puisqu'il suffisait, pour ce faire, de continuer à naviguer sur le site web, sans qu'aucune autre démarche ne soit nécessaire dans le chef des utilisateurs. Pour renforcer sa défense, la société chinoise prétend s'être de la sorte conformée à la recommandation de la CNIL qui prévoit, en son article 2, que «toute inaction ou action des utilisateurs autre qu'un acte positif signifiant son consentement doit être interprétée comme un refus de consentir ; dans ce cas, aucune opération de lecture ou d'écriture soumise au consentement ne peut légalement avoir lieu»⁴⁹.

Cet argument est l'occasion, pour la CNIL, de préciser et d'affiner ses exigences concernant la forme du consentement, mais également la forme du refus. Elle rappelle en effet que si un refus implicite au dépôt de cookies est possible et toléré, c'est uniquement dans l'hypothèse où les utilisateurs sont pleinement conscients des conséquences de leur inaction parce qu'ils ont reçu une information complète en ce sens⁵⁰. Or, en l'espèce, la bannière de cookies telle qu'elle était présente sur le site web ne fournissait aucune information aux utilisateurs sur la manière de refuser les cookies. La CNIL renonce dès lors à suivre cette argumentation

et souligne qu'en pratique, cette manière de procéder implique un déséquilibre entre les modalités d'acceptation et de rejet poussant indirectement les utilisateurs du site web à choisir d'accepter le dépôt des cookies. Ce déséquilibre en faveur de l'acceptation se matérialise de plusieurs façons.

Premièrement, la CNIL relève le caractère peu intuitif de la bannière de cookies qui n'indique aucunement aux utilisateurs la possibilité de poursuivre la navigation sur le site web sans poser de choix explicite sur la bannière, soit en cliquant sur «Tout accepter», soit en cliquant sur le bouton «Gérer les paramètres» pour pouvoir par la suite refuser le dépôt des cookies. De surcroît, à défaut de choix explicite, la bannière de cookies restait de manière persistante tout au long de la navigation⁵¹. Or, comme la CNIL l'avait déjà précisé dans sa recommandation, la persistance d'un bandeau de cookies implique un inconfort de navigation qui pousse les utilisateurs à poser un choix explicite quant au dépôt des cookies afin de la faire disparaître la plus rapidement possible⁵². En l'espèce, l'utilisateur était alors fortement incité à cliquer sur le bouton «Tout accepter», cette solution étant la plus simple et la plus rapide⁵³.

Deuxièmement, la décision souligne le caractère peu explicite du bouton «Gérer les paramètres» – présent à côté du bouton «Tout accepter» – qui n'indique nullement qu'il permet, au terme de trois actions subséquentes, d'aboutir à un refus des cookies. Par conséquent, cela peut créer une confusion dans le chef des utilisateurs et leur laisser penser qu'il n'est en fait pas possible de refuser le dépôt de cookies⁵⁴.

⁴⁸ Décision «TikTok», point 68.

⁴⁹ Décision «TikTok», point 68 ; recommandation de la CNIL du 17 septembre 2020, art. 2.

⁵⁰ *Idem*, point 70.

⁵¹ *Idem*, point 71.

⁵² Recommandation de la CNIL du 17 septembre 2020, *op. cit.*, point 36.

⁵³ Décision «TikTok», point 71.

⁵⁴ *Idem*, point 72.

Ces deux constats, combinés au fait qu'une navigation sur internet se caractérise par la rapidité et la fluidité, impliquent qu'en pratique, les utilisateurs, pressés de voir cette bannière de cookies disparaître afin d'obtenir un certain confort de navigation, étaient clairement incités à favoriser l'acceptation des cookies – même si *ab initio*, ils auraient souhaité les refuser⁵⁵.

En définitive, s'il était théoriquement possible, pour les utilisateurs du site web, de refuser le dépôt des cookies – soit en continuant à naviguer, soit en suivant le parcours en trois clics – il apparaît que les modalités mises en place par TikTok étaient telles qu'elles rendaient le refus plus fastidieux que l'acceptation, ce qui avait pour conséquence de décourager les utilisateurs à refuser les cookies et, à l'inverse, de les inciter à privilégier la facilité du bouton «Tout accepter». La CNIL conclut dès lors que le consentement ne pouvait pas être considéré comme étant valablement recueilli⁵⁶.

Forte de son interprétation du caractère libre du consentement⁵⁷, la CNIL en vient à établir des exigences particulières liées à la forme du refus. Le refus implicite est valable uniquement si les utilisateurs ont reçu une information complète les informant des conséquences de leur silence. Le refus implicite semble dès lors devoir être «éclairé». À défaut, un refus explicite, se présentant sous la forme d'un «acte positif clair» semble requis, celui-ci devant pouvoir être manifesté avec la même facilité que l'octroi du consentement⁵⁸.

Du côté du groupe de travail instauré au sein du CEPD, il ressort du rapport que la question de

l'absence de bouton «Tout refuser» ou «Rejeter les cookies» au premier niveau – sur la bannière de cookies – n'a pas fait l'objet d'un consensus entre les différentes autorités de protection des données. Le comité indique en effet qu'alors que la majorité des autorités de protection des données consultées condamne cette pratique, certaines autorités considèrent qu'elles ne peuvent pas retenir un manquement sur la base de l'article 5, § 3, de la directive ePrivacy dans la mesure où cet article ne requiert pas un refus explicite pour le dépôt des cookies⁵⁹. Malgré cette absence d'unanimité sur la nécessité de prévoir un bouton «Tout refuser» au même niveau que le bouton «Tout accepter», le groupe de travail européen condamne les bannières de cookies qui donnent l'impression aux utilisateurs de devoir donner leur consentement au dépôt de cookies ou qui incitent clairement l'utilisateur à donner son consentement⁶⁰. Pour illustrer ses propos, le CEPD donne notamment l'exemple d'une bannière de cookies qui contiendrait un bouton «Tout accepter», avec comme seule alternative, un lien contenant les mots «Tout refuser» ou «Continuer sans accepter» qui serait présent en dehors de la bannière de cookies⁶¹.

Si le CEPD est donc moins explicite que la CNIL sur ce qui est effectivement attendu de la part des acteurs du web, force est de constater que leur idéal de bannière de cookies semble sensiblement similaire.

D. Le caractère éclairé du consentement : vers un devoir d'information affiné

Lors du contrôle réalisé par la CNIL, il est également apparu que l'information fournie par TikTok à ses utilisateurs concernant les cookies était insuffisante à plusieurs égards.

⁵⁵ Décision «TikTok», point 74.

⁵⁶ *Idem*, points 74 et 77.

⁵⁷ Nous faisons référence à l'interprétation de la CNIL selon laquelle il doit être aussi aisé de refuser les cookies que de les refuser (recommandation de la CNIL du 17 septembre 2020, *op. cit.*, point 30).

⁵⁸ Voy. à cet égard : recommandation de la CNIL du 17 septembre 2020, *op. cit.*, point 33.

⁵⁹ EDPB, «Report of the work undertaken by the Cookie Banner Taskforce», *op. cit.*, points 6-8.

⁶⁰ *Idem*, point 13.

⁶¹ *Idem*, point 14.

Outre le caractère libre, le consentement au dépôt des cookies doit également être éclairé, c'est-à-dire donné par les utilisateurs en pleine connaissance de cause. Cette qualité est directement liée au devoir d'information pesant sur les organismes souhaitant déposer des cookies et leur imposant, notamment, de fournir aux utilisateurs une information claire et complète sur les finalités poursuivies par le dépôt de cookies sur les terminaux utilisés⁶².

Il ressort des constats réalisés par la rapporteuse que la bannière de cookies telle qu'elle apparaissait au moment du contrôle sur le site de la société, informait les utilisateurs de l'utilisation de cookies par TikTok, notamment « à des fins d'analyse et de marketing » ou encore « afin d'améliorer l'expérience sur le site web »⁶³. En outre, le bouton « Gérer les paramètres » permettant aux utilisateurs de marquer leur refus et/ou leur consentement de manière distincte et spécifique pour chaque cookie, reprenait la liste des cookies avec à nouveau, comme seule indication concernant la finalité,

le fait qu'il s'agissait de « cookies d'analyse ou de marketing »⁶⁴.

La CNIL rappelle que l'information fournie aux utilisateurs au premier niveau – dans la bannière de cookies – doit être suffisamment claire et précise pour permettre à l'utilisateur du site web de faire un choix éclairé dès ce stade⁶⁵. Or, en l'espèce, l'autorité de protection des données française met en exergue le caractère approximatif et général de l'information communiquée et retient un premier motif de violation de l'obligation d'information⁶⁶. Ainsi, elle souligne le caractère particulièrement vague du terme « à des fins de marketing », qui peut recouvrir des réalités multiples et variées, telles que des cookies installés à des fins de statistiques pour mesurer l'audience de la publicité affichée, à des fins de prospection commerciale, ou encore à des fins de publicité ciblée⁶⁷. Or, un utilisateur disposé à accepter des cookies statistiques destinés à mesurer l'audience du site consulté pourrait en revanche être plus réticent à consentir à des cookies installés afin de pouvoir lui soumettre de la publicité ciblée⁶⁸.

Pour la même raison, la CNIL a conclu à une seconde violation du devoir d'information par TikTok concernant l'information fournie

⁶² Article 5, § 3, de la directive 2002/58/CE (directive « ePrivacy ») : « Les États membres garantissent que l'utilisation des réseaux de communications électroniques en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur ne soit permise qu'à condition que l'abonné ou l'utilisateur soit muni, dans le respect de la directive 95/46/CE, d'une information claire et complète, entre autres sur les finalités du traitement, et que l'abonné ou l'utilisateur ait le droit de refuser un tel traitement par le responsable du traitement des données. (...) ». Article 82 de la loi Informatique et Libertés : « Tout abonné ou utilisateur d'un service de communications électroniques doit être informé *de manière claire et complète*, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant : 1. De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son terminal de communications électroniques, ou à inscrire des informations dans cet équipement ; 2. Des moyens dont il dispose pour s'y opposer. (...) ».

⁶³ Décision « TikTok », point 80.

⁶⁴ *Idem*.

⁶⁵ *Idem*, point 85.

⁶⁶ *Idem*, point 83.

⁶⁷ *Idem*, point 84.

⁶⁸ Voy. à ce sujet les résultats de l'enquête « Les Français et la réglementation en matière de cookies » menée par l'Ifop et la CNIL, p. 16 qui indique que 59 % des Français interrogés sont prêts à consentir au dépôt de cookies permettant au site de collecter des données afin de mesurer son audience plus précisément, alors que 44 % sont prêts à consentir à des cookies permettant au site web d'afficher des publicités personnalisées en fonction des comportements de navigation. Cette enquête est disponible sur le site web de la CNIL à l'adresse suivante : https://www.cnil.fr/sites/default/files/atoms/files/les_francais_et_la_reglementation_en_matiere_de_cookies_-_sondage_ifop_pour_la_cnil_-_decembre_2019_.pdf.

à un second niveau, lorsque les utilisateurs consultent l'interface de recueil du consentement où est repris, isolément, chacun des cookies. Elle considère que l'information fournie est à nouveau trop vague et incomplète. En effet, celle-ci n'indique pas de manière suffisamment précise la finalité propre à chaque cookie, tous étant repris sous la forme d'un *listing* sous l'intitulé générique «cookies d'analyse et de marketing». La CNIL relève, dès lors, que l'analyse et le marketing sont deux finalités de nature distincte, et qu'il convient non seulement de distinguer les cookies qui relèvent de l'analyse et ceux qui relèvent du marketing, mais qu'il importe également de préciser ces finalités qui restent, même prises séparément, trop imprécises, en indiquant, pour chaque cookie, la finalité effectivement poursuivie⁶⁹.

Notons que la CNIL avait déjà communiqué en détail sur ce devoir d'information dans sa recommandation, dans laquelle elle avait fourni un exemple du niveau de précision attendu dans la définition des finalités poursuivies par les cookies⁷⁰. Dans cet exemple, elle indique que la finalité de «publicité» est en elle-même insuffisante, celle-ci devant être affinée et précisée en signalant explicitement le rôle effectivement joué par chaque traceur publicitaire, en mentionnant que les traceurs permettant de réaliser de la publicité ciblée doivent être annoncés à travers la finalité «publicité personnalisée», ou encore que les cookies destinés à localiser le terminal de l'utilisateur afin de lui fournir une publicité adaptée à sa localisation doivent être annoncés à travers la finalité «publicité géolocalisée»⁷¹.

Concernant le devoir d'information, ce n'est donc pas tant sur la forme utilisée que TikTok

est sanctionné⁷², mais bien sur le fond, les termes utilisés pour informer les utilisateurs étant trop génériques et trop imprécis et ne permettant effectivement pas aux utilisateurs de comprendre la portée des cookies vis-à-vis desquels ils devaient se positionner. L'objectif poursuivi par la CNIL est finalement semblable à celui poursuivi dans son analyse relative au caractère libre du consentement: empêcher les acteurs du web d'influencer le comportement des utilisateurs en se cachant derrière des termes génériques créant une confusion potentielle et masquant, dans une certaine mesure, le but réellement poursuivi par les cookies à accepter.

V. LA SANCTION

Par cette décision, la CNIL prononce sa première sanction à l'encontre de TikTok. Celle-ci prend la forme d'une amende de cinq millions d'euros. L'occasion, pour l'autorité de protection des données française, d'asseoir à nouveau sa position concernant la problématique des cookies en montrant qu'il s'agit d'un secteur dans lequel elle est désormais intransigeante.

Alors que TikTok faisait valoir qu'une amende était, au vu des manquements reprochés, disproportionnée et qu'un simple rappel à l'ordre était suffisant⁷³, la CNIL, quant à elle, insiste sur la gravité des manquements constatés pour justifier l'amende infligée⁷⁴.

Trois éléments sont particulièrement intéressants dans la justification apportée par la CNIL. Premièrement, la CNIL a tenu compte

⁶⁹ Décision «TikTok», point 86.

⁷⁰ Recommandation de la CNIL du 17 septembre 2020, *op. cit.*, article 2.1, p. 3.

⁷¹ *Idem*.

⁷² En effet, comme l'a relevé TikTok dans sa défense, une information, bien qu'incomplète, était fournie aux utilisateurs tant au premier niveau sur la bannière des cookies qu'au second niveau dans la politique de cookies ainsi que dans l'interface de recueil des consentements.

⁷³ Décision «TikTok», point 90.

⁷⁴ *Idem*, point 92.

du nombre de traitements illégaux réalisés en raison de la masse d'utilisateurs du site web⁷⁵. Deuxièmement, une part non négligeable du public est composée d'adolescents (38% des utilisateurs ont entre 13 et 17 ans). La CNIL retient le besoin d'une protection renforcée pour ces utilisateurs plus vulnérables⁷⁶. Troisièmement, la CNIL justifie également l'imposition d'une amende par le fait que jusqu'à la fin du mois de février 2022, il n'était pas possible, sur le site web de TikTok, de refuser les cookies avec la même facilité que le fait de les accepter, alors qu'elle avait laissé aux acteurs du web un délai courant jusqu'au 1^{er} avril pour se mettre en conformité⁷⁷. La CNIL précise qu'avant cette date butoir, elle a suffisamment communiqué sur l'importance de ce principe et sur les modalités pratiques qu'il convenait de mettre en place afin de s'y conformer. Le fait que TikTok ait collaboré avec les services de la CNIL tout au long de la procédure ainsi que le fait que TikTok se soit désormais mise en conformité en ajoutant, sur la bannière de cookies, un bouton «Tout refuser» au même niveau que le bouton «Tout accepter», n'ont pas été reconnues comme des circonstances atténuantes dans son chef⁷⁸.

VI. LA CHASSE AUX «*DARK PATTERNS*» ET UNE RECONNAISSANCE CROISSANTE DU PRINCIPE D'«*AUTONOMIE INDIVIDUELLE*»

En philosophie, l'autonomie individuelle est parfois définie comme étant «la capacité à se gouverner soi-même, sans faire appel à une source de commandement extérieure ou à une autorité transcendante»⁷⁹. L'autonomie individuelle est donc directement liée à la liberté

d'autodétermination, c'est-à-dire la possibilité de faire des choix par soi-même.

Le développement de l'informatique et d'une société de l'information s'est accompagné, dès l'origine, de craintes pour la vie privée des individus, notamment quant à la gestion de leurs données à caractère personnel⁸⁰. S'est alors développé le concept «d'autodétermination informationnelle»⁸¹, qui fait référence «à la possibilité de contrôler ses propres informations personnelles, c'est-à-dire le droit des individus de déterminer quelles informations les concernant peuvent être communiquées à qui et à quelles fins», étant entendu que la notion de «contrôle» se réfère davantage au droit d'être dûment informé de l'usage qui est fait des données plutôt qu'à un réel pouvoir de décision quant à ces données dans le chef des individus⁸². Ce principe étant indispensable afin de garantir une protection effective de la vie privée des individus, il s'est exprimé implicitement dans la réglementation européenne en matière de vie privée, à travers une série de droits et de principes destinés à garantir aux individus un certain contrôle dans la gestion de leurs données⁸³. Figurent notamment au rang de ces droits et principes, les principes de loyauté et de transparence, le droit à l'accès

⁸⁰ Pour une analyse détaillée de la problématique de l'information dans le secteur public dans la société de l'information, voy. la thèse de C. DE TERWANGNE, *Société de l'information et mission publique d'information*, FUNDP, Faculté de droit, 2000.

⁸¹ C. DE TERWANGNE, «Chapitre 3: Droit à l'oubli, droit à l'effacement ou droit au déréférencement? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique», in *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 246.

⁸² C. DE TERWANGNE, *op. cit.*, p. 246; S. VERGNOLLE, *L'effectivité de la protection des personnes par le droit des données à caractère personnel*, Bruxelles, Bruylant, 2022, p. 320.

⁸³ T. TOMBAL, «Chapitre 2: Les limitations aux droits de la personne concernée», in *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Larcier, 2018, p. 555.

⁷⁵ *Idem*, point 93.

⁷⁶ *Idem*, point 94.

⁷⁷ *Idem*, point 98.

⁷⁸ *Idem*, point 96.

⁷⁹ R. MONJO, «L'autonomie, de l'indépendance vers l'interdépendance», *Le sociographe*, 2013/5, p. 173.

aux données ou, plus récemment, la reconnaissance explicite du droit à l'oubli dans le RGPD⁸⁴.

Les développements récents des technologies numériques – tels que l'usage constant de smartphones, d'objets connectés ou de réseaux sociaux – ont contribué à créer un environnement numérique fondé sur le traitement massif de données et la personnalisation des contenus⁸⁵. Cette situation s'est accompagnée de nouvelles menaces pour l'autonomie individuelle, notamment le risque d'être soumis à des manipulations et à des pressions extérieures⁸⁶. L'environnement numérique présente en effet ces particularités de rendre les manipulations beaucoup moins visibles et tangibles que dans le monde physique⁸⁷ et de pouvoir être modulé presque entièrement en vue d'exercer une influence sur le comportement des utilisateurs⁸⁸. Outre la conformité au cadre européen, la lutte contre les bannières de cookies conçues en vue d'obtenir rapidement et facilement le consentement des internautes témoigne également du souci d'accroître l'autonomie individuelle des individus, soit le droit, pour chacun, de prendre des décisions en pleine autonomie, sans faire l'objet de manipulation ou de contrainte⁸⁹. En matière de protection de la vie privée et des données à caractère personnel, c'est à nouveau implicitement que la notion d'autonomie individuelle et l'interdiction de recourir à des manœuvres manipulatoires et trompeuses trouvent écho dans le droit positif, initialement à travers les applications et les interprétations des concepts de consentement libre et éclairé,

et plus récemment, à travers l'attention particulière et grandissante qu'octroient les autorités de protection des données nationales ainsi que les organes consultatifs à la problématique des *dark patterns*.

Alors qu'en droit de la consommation, l'interdiction, pour les entreprises, de recourir à des pratiques trompeuses et manipulatoires envers les consommateurs est prévue explicitement dans la législation européenne depuis l'adoption de la directive (CE) 2005/29⁹⁰, l'interdiction des pratiques trompeuses et manipulatoires et la reconnaissance explicite de l'autonomie individuelle se retrouvent désormais également dans les nouvelles réglementations européennes en matière de services technologiques et numériques. En témoigne l'article 6 de la proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données qui est destiné à prévoir un cadre réglementaire harmonisé au sein de l'Union européenne pour les échanges de données dans les secteurs économiques et industriels⁹¹. Cet article prévoit que «le tiers s'abstient de contraindre, tromper ou manipuler l'utilisateur de quelque manière que ce soit, en nuisant ou en portant atteinte à l'autonomie, à la prise de décision ou aux choix de l'utilisateur, y compris au moyen d'une interface numérique avec l'utilisateur». De la même

⁸⁴ S. VERGNOLLE, *op. cit.*, p. 345; C. DE TERWANGNE, *op. cit.*, p. 247.

⁸⁵ S. VERGNOLLE, *op. cit.*, pp. 322-323.

⁸⁶ *Idem*, p. 320.

⁸⁷ *Idem*, pp. 326 et 330; E. MIK, *op. cit.*, pp. 11 et 12.

⁸⁸ E. MIK, *op. cit.*, pp. 11-12.

⁸⁹ M. GARTNER, «Regulatory Acknowledgment of Individual Autonomy in European Digital Legislation: From Meta-Principle to Explicit Protection in the Data Act», *European Data Protection Law Review*, n° 4/2022, p. 466.

⁹⁰ Directive (CE) 2005/29 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 et modifiant la directive 84/450/CEE et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil («directive sur les pratiques commerciales déloyales»), *J.O.*, L 149/22, 11 juin 2005.

⁹¹ Proposition de règlement européen du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), COM (2022) 68 final.

manière, la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle⁹², prévoit, en son considérant 16, que «des techniques de manipulation fondées sur l'IA peuvent être utilisées pour persuader des personnes d'adopter des comportements indésirables ou pour les tromper en les poussant à prendre des décisions d'une manière qui met à mal et compromet leur autonomie, leur libre arbitre, et leur liberté de choix. La mise sur le marché, la mise en service ou l'utilisation de certains systèmes d'IA qui altèrent substantiellement les comportements humains d'une manière qui est susceptible de causer un préjudice psychologique ou physique sont particulièrement dangereuses et devraient être interdites»⁹³. Enfin, en ce qui concerne plus spécifiquement la conception et l'organisation des interfaces en ligne, l'article 25 du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques⁹⁴ prévoit que «les fournisseurs de plateformes en ligne ne conçoivent, n'organisent ni n'exploitent leurs interfaces en ligne de façon à tromper ou à manipuler les destinataires de leur service ou de toute autre façon propre à altérer ou à entraver substantiellement la capacité des destinataires de leur service à prendre des décisions libres et éclairées»⁹⁵.

Si ces propositions de réglementation ne concernent pas directement le secteur de la protection de la vie privée, force est de constater que ces questions liées à l'autodétermination prennent davantage d'ampleur dans le droit positif en faisant désormais l'objet d'une reconnaissance explicite par le législateur européen et en y incluant une interdiction explicite des pratiques trompeuses et manipulatoires. La reconnaissance d'un droit à l'autodétermination semble en effet primordiale pour garantir l'autonomie des individus qui peut être bousculée par l'omniprésence des technologies et le développement constant du secteur numérique. On peut à cet égard regretter que la proposition de règlement ePrivacy, qui est destinée à abroger et à remplacer le cadre législatif actuel, ne contienne aucune référence explicite à l'autonomie individuelle des individus ainsi qu'à l'interdiction des pratiques manipulatoires et trompeuses dans le secteur des communications électroniques. Dans ce contexte, c'est donc aux autorités de protection des données nationales, accompagnées par le CEPD, qu'il revient de continuer à combler cette lacune réglementaire en continuant à interpréter et à renforcer les principes contenus dans le RGPD et dans la directive ePrivacy.

VII. CONCLUSION

Les technologies numériques présentent cette particularité qu'elles permettent à la fois de respecter – en apparence – une norme légale, tout en étant pensées et configurées afin de favoriser les intérêts économiques du responsable du traitement.

En matière de cookies, la CNIL l'a bien compris et entend profiter de sa compétence désormais bien établie pour sanctionner massivement les géants du web qui, en matière de protection des données, échappent le plus souvent à sa compétence au profit de l'Autorité de protec-

⁹² Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle), COM 2021/206 final.

⁹³ Le Titre II de la proposition d'IA Act contient un article 5 qui reprend les différentes pratiques interdites en matière d'intelligence artificielle et auquel nous renvoyons pour de plus amples détails.

⁹⁴ Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive (CE) 2000/31 (règlement sur les services numériques), J.O., L 277/1, 27 octobre 2022.

⁹⁵ Voy. également en ce sens le considérant 67 du règlement (UE) 2022/2065 sur les services numériques.

tion des données irlandaise. Après Google, Apple, Facebook, Amazon et Microsoft, c'était désormais au tour de TikTok de répondre de ses manquements devant l'Autorité de protection des données française.

Si les thématiques abordées par la CNIL dans sa décision sont sans véritable surprise – celle-ci reprenant les thématiques traditionnellement traitées par la formation restreinte dans d'autres décisions rendues en matière de cookies – les circonstances propres à ce cas d'espèce ont été l'occasion de préciser ses exigences et d'affiner les contours de la réglementation en ayant l'occasion de contredire, en droit, un nouvel argument soulevé par TikTok: le fait de permettre aux utilisateurs de refuser le dépôt des cookies en continuant à naviguer sur le site web sans

les informer que cette poursuite de navigation équivaut à un refus crée un déséquilibre en faveur de l'acceptation, ce qui porte atteinte à la liberté du consentement.

Au fil de ses décisions, la CNIL reste vigilante en affinant son interprétation des conditions requises pour obtenir un consentement valable. À l'issue de cette salve de décisions, concluons que la CNIL a réduit à peau de chagrin les possibilités, pour les acteurs du web, de contourner leurs obligations à travers des bannières de cookies qui biaisent le consentement des utilisateurs, au profit d'une protection accrue de la protection de la vie privée et de l'autonomie individuelle des utilisateurs.

Alix GOBERT