Jean-Claude Bonichot

DONNÉES PERSONNELLES : L'INVENTION EUROPÉENNE D'UN MONDE NOUVEAU

En répondant à Elon Musk, qui s'était écrié « L'oiseau est libéré » après avoir racheté Twitter pour la modique somme de 44 milliards de dollars, « En Europe, l'oiseau volera selon nos règles européennes », le commissaire européen chargé du numérique, Thierry Breton, a parfaitement résumé la situation : l'Union européenne s'est dotée d'un droit du numérique, d'un droit propre au numérique, d'un droit « dur » – puisque aussi bien aujourd'hui il faut préciser… – qui envisage la matière sous tous ses aspects et prévoit des moyens efficaces pour en assurer correctement l'application.

Il s'agit là d'un choix « continental » qui correspond à la conception européenne du monde 2.0 ou 3.0 dans lequel nous vivons désormais. Celle-ci repose sur cette idée simple que non seulement l'économie du numérique ne saurait se développer en dehors de la règle de droit, mais encore qu'elle est subordonnée aux valeurs qui informent la société européenne, au nombre desquelles le respect de la vie privée et la protection des données personnelles.

Dans un monde où l'attitude vis-à-vis de cette société en perpétuelle évolution est très différente d'un continent à l'autre, l'Union européenne est sans doute une exception. Mais ce que les Américains appellent « *the Bloc* » a le droit d'avoir sa philosophie propre des nouvelles technologies de l'information (NTI) et les moyens de la faire vivre. L'évolution de la matière en ce début des années 2020 le montre d'ailleurs : d'une part en adoptant des règlements plutôt que des directives, d'autre part en prévoyant que les règles de l'Union s'appliqueraient à toute entreprise qui a avec elle un « lien étroit » même si elle

n'y est pas établie, l'Union a fait un pas vers plus d'intégration et plus d'exterritorialité[1].

Il y a bien longtemps déjà que l'Union s'est dotée d'un instrument de protection des données personnelles et, plus généralement, de régulation du secteur des NTI avec la directive 95/49/CE, du 24 octobre 1995, qui était l'équivalent de notre loi « informatique et libertés », du 6 janvier 1978. La Charte des droits fondamentaux de l'Union européenne – dont il faut rappeler qu'elle a la même valeur que les traités – a consacré cette orientation : elle a mis au rang des droits fondamentaux non seulement la classique protection de la vie privée et familiale et des communications (art. 7), mais aussi celle des données personnelles (art. 8). Il s'agit là d'un choix capital même s'il nous paraît assez naturel, à nous, Européens. La protection des données

et tout ce qu'elle implique sont mis au rang des droits de l'homme au même titre que la liberté ou la sûreté, ou la liberté de conscience. La Cour de justice de l'Union européenne a tiré de ces règles toutes leurs conséquences.

Le droit de l'Union est donc l'expression d'une politique européenne claire : les NTI et les entreprises du secteur sont soumises aux valeurs de l'Union européenne ; celles-ci sont protégées par des instruments efficaces et sans équivalent dans le reste du monde ; il en résulte un véritable statut de l'utilisateur et en particulier de l'internaute.

Une orientation politique : la subordination aux valeurs de l'Union

Que les droits et libertés doivent être protégés contre la puissance publique n'est pas nouveau et explique tout le régime de ce qu'on appelait « les libertés publiques ». La marche de nos sociétés montre toutefois aujourd'hui plus que jamais qu'ils doivent aussi être protégés contre les pouvoirs privés. Ainsi, la Cour de justice a certes rendu de grands arrêts à propos des interventions des États membres vis-à-vis des données personnelles et en particulier de leur rétention dans un but de sécurité publique, depuis l'arrêt *Digital Rights* en 2014[2], en passant

1. Pour une vue d'ensemble de la jurisprudence de la CJUE sur les NTI, cf. mon ouvrage *La Cour de justice de l'Union européenne*, Paris, Dalloz, 2021, p. 269 et suiv. ; cf. aussi Maciej Szpunar, « Territoriality of Union Law in the Era of Globalisation », in *Évolution des rapports entre les ordres juridiques de l'Union européenne, international et nationaux. Liber amicorum Jiří Malenovský*, Bruxelles, Bruylant, 2020, p. 149-168.

2. C-293/12 et C-594/12.

par l'arrêt *Tele2 Sverige* en 2016[3], jusqu'aux arrêts *La Quadrature du Net*[4] et *Privacy International* en 2020[5], ainsi que *Commisioner of the Garda Síochána* en 2022[6]. Elle y a manifesté une hostilité de principe à tout système de rétention généralisée des données de trafic. Mais les multiples arrêts qu'elle a été amenée à rendre à propos des entreprises du Net traduisent fort bien aussi la vision européenne des NTI qui les subordonne clairement aux valeurs inscrites dans la Charte. Cette conception s'exprime dans le règlement général sur la protection des données, qui a remplacé en 2016 la directive de 1995 et constitue incontestablement l'instrument le plus exigeant au monde dans ce domaine.

Le « RGPD »[7] met en œuvre les principes définis par la Charte : loyauté des traitements sur la base du consentement des intéressés ou en vertu de la loi ; droit d'accès aux données et contrôle d'une autorité indépendante. Son champ d'application est large puisqu'il concerne non seulement les opérateurs établis dans l'Union mais aussi ceux qui y offrent leurs services ou y suivent le comportement de personnes. Il décline les obligations de licéité, loyauté, transparence, proportionnalité et sécurité. Il prévoit des règles précises pour l'accès aux données et leur effacement, ainsi que pour le retrait du consentement à ce que des données personnelles soient traitées. Il fixe un régime contraignant aux transferts de données vers des États tiers ou des organisations internationales. Il prévoit l'existence dans chaque État membre d'une autorité indépendante de contrôle à laquelle peuvent être adressées des réclamations. À cet égard, il n'est pas indifférent de remarquer que le Conseil d'État français vient de juger que l'examen de sa réclamation par un plaignant est un droit, ce qui implique que le refus d'y donner suite soit motivé[8]. Ces autorités jouent un rôle essentiel dans le système européen des NTI : chargées d'assurer le respect du règlement en coopérant avec les autorités des autres États membres, elles peuvent imposer aux entreprises des mesures correctrices et sont investies d'un pouvoir de sanction qui, selon le cas, peut aller jusqu'à 2 %, voire 4 % du chiffre d'affaires mondial. La CNIL française a ainsi infligé, en octobre 2021, une amende de 150 millions d'euros à Google

3. C-203/15.
4. C-511/18, C-512/18 et C-520-18.
5. C-623/17.
6. C-140/20. Cf. aussi l'arrêt du 21 juin 2022, *Ligue des droits humains*, C-817/19, à propos des données des passagers aériens.
7. Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (*JOUE*, L 119/1, 4 mai 2016).
8. CE, 21 octobre 2022, *Mme Pouliou*, n° 459254.

en raison de l'impossibilité pour ses clients de refuser des cookies et une autre, en décembre 2022, de 60 millions à Microsoft pour ne pas permettre aussi facilement de refuser les cookies que de les accepter. De même, la maison mère de Facebook, Meta, s'est-elle vu infliger, en juillet précédent, une amende de 265 millions par le régulateur irlandais pour ne pas avoir suffisamment protégé les données de plus de cinq cents millions d'utilisateurs qui ont été piratées.

La Cour de justice a fait de l'indépendance de ces autorités de régulation un principe cardinal du droit européen des NTI. Ainsi a-t-elle considéré que la tutelle exercée en Allemagne sur les autorités chargées dans les *Länder* de la protection des données était incompatible avec la législation de l'Union et qu'il en allait de même pour l'autorité autrichienne, jugée trop proche des services centraux de l'État[9]. Dans la même ligne,
100 la Cour juge que les délégués à la protection des données que certaines entreprises sont tenues de désigner, en vertu de l'article 38 du RGPD, doivent être protégés contre toute pression qui serait liée à l'exercice de leurs fonctions et que les États membres peuvent avoir une législation encore plus protectrice, notamment en matière de licenciement[10].

Des instruments efficaces ? L'encadrement des géants du Net

L'affirmation des principes de l'Union a été complétée en 2022 par un ensemble de règles qui ont fait beaucoup de bruit et sont destinées à encadrer et discipliner le marché des NTI, pour tenir compte des caractères particuliers qui sont les siens et rendent difficile d'appréhender des comportements critiquables avec les instruments classiques du droit de la concurrence ou du droit de la consommation.

Le cadre fixé par le législateur de l'Union a été tracé dans un souci d'équilibre. La navigation est en effet difficile entre l'impératif de tenir compte des réalités d'aujourd'hui, qui font que la liberté de communication passe par les NTI, et les enjeux économiques et commerciaux, qui font que le monde du Net démultiplie les possibilités de pratiques déloyales ou même de fraude. Ainsi le Conseil constitutionnel a-t-il récemment rappelé : « En l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au

9. CJUE, 9 mars 2010, *Commission c. Allemagne*, C-518/07, et 16 octobre 2012, *Commission c. Autriche*, C-614/10.

10. CJUE, 22 juin 2022, *Leistritz AG*, C-534/20.

public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services et de s'y exprimer[11]. »

L'Union européenne s'est dotée d'un instrument que l'on pourrait qualifier de « droit spécial de la concurrence » afin de réguler le secteur des *services de plateforme essentiels*, c'est-à-dire ceux qui font de nos jours le quotidien de la population : moteurs de recherche, réseaux sociaux, partages de vidéos, navigateurs. C'est l'objet du règlement 2022/1925, du 14 septembre 2022[12]. Il est, selon le langage abscons qu'il est désormais d'usage d'employer, « relatif aux marchés contestables et équitables » dans le secteur numérique. Cela signifie qu'il a pour but d'assurer la loyauté des relations commerciales entre les entreprises et avec les consommateurs finaux, et de permettre que joue une véritable concurrence dans un domaine où les moyens de verrouiller l'accès au marché ou de favoriser ses propres produits sont légion et évoluent constamment.

Le règlement s'applique aux *contrôleurs d'accès*, c'est-à-dire aux entreprises de plateforme en quelque sorte installées dans le paysage et qui ont un poids tel qu'elles peuvent empêcher d'autres entreprises de proposer leurs services ou abuser de leur position. L'idée est que le droit de la concurrence seul ne permet pas de les encadrer de manière suffisamment efficace.

Il appartient à la Commission européenne d'en dresser la liste. Sont désignées comme contrôleur d'accès celles qui répondent à une triple condition de poids économique dans le marché intérieur, de large clientèle et de stabilité dans cette position[13]. Les entreprises ainsi désignées sont soumises à des obligations particulières, nombreuses et détaillées notamment en matière de protection des données personnelles, afin qu'elles n'entravent pas le développement d'autres entreprises ou ne favorisent pas leurs propres activités, ou encore pour assurer l'interopérabilité.

La Commission est exclusivement compétente pour assurer le respect du règlement. Non seulement lui appartient-il de qualifier une plateforme de contrôleur d'accès, mais elle dispose de pouvoirs d'enquête,

11. Décision 1016 QPC du 21 octobre 2022.

12. *JOUE*, L 265/1, 12 octobre 2022.

13. Chiffre d'affaires d'au moins 7,5 milliards d'euros ou capitalisation d'au moins 75 milliards ; au moins quarante-cinq millions d'utilisateurs finaux ou dix mille entreprises ; réalisation de ces conditions au cours des trois derniers exercices. Le règlement, dans son article 13, prévoit un dispositif anti-contournement, par exemple dans le cas où l'entreprise en cause fragmenterait ses activités.

d'inspection, peut demander des renseignements dans des conditions comparables aux pouvoirs en matière de concurrence. Elle dispose d'un important pouvoir de sanction qui peut aller jusqu'à 10 % du chiffre d'affaires mondial et même 20 % en cas de récidive. Elle peut aussi infliger une amende de 1 % du chiffre d'affaires en cas de défaut de coopération, ainsi que des astreintes. La Cour de justice est dotée par le règlement, comme le permet l'article 261 du traité sur le fonctionnement de l'Union, d'un pouvoir de pleine juridiction. Le règlement comporte des règles pour coordonner l'exercice par la Commission de ses pouvoirs avec ceux des autorités nationales de concurrence, étant entendu que le droit européen et national de la concurrence continue à s'appliquer. Il prévoit aussi que la Commission a le droit d'intervenir devant les juridictions nationales.

102 Le règlement 2022/1925 vient ainsi compléter le droit classique de la concurrence afin de tenir compte des spécificités des grandes plateformes, déjà bien mises en évidence par le Conseil d'État français dans son étude annuelle de 2017[14], et de leur modèle d'affaires, qui les conduit par le jeu d'intégrations verticales à faire le ménage autour d'elles[15]. La Cour de justice de l'Union européenne est d'ailleurs actuellement saisie de la question de savoir comment se combinent les règles de concurrence et celles relatives à la protection des données personnelles. L'Oberlandesgericht de Düsseldorf, tribunal supérieur du *Land*, dans le cadre d'un litige qui oppose Meta à l'autorité de concurrence allemande, lui a demandé si, afin de décider s'il y a abus de position dominante, une autorité nationale de concurrence peut appliquer le RGPD et en constater une violation par les clauses contractuelles de l'entreprise. L'avocat général Rantos a rendu ses conclusions le 20 septembre 2022 et proposé de répondre par l'affirmative et que l'autorité de concurrence devait tenir compte des positions déjà prises par l'autorité nationale chargée de l'application du RGPD et, le cas échéant, la consulter.

Second instrument majeur : le tout récent règlement « relatif à un marché unique des services numériques », ou *Digital Services Act* (*DSA*), constituera, à compter du 17 février 2024, la charte de base des entreprises de NTI dans l'Union européenne. Il harmonise la plupart des règles régissant les services

14. *Puissance publique et plateformes numériques : accompagner l'« ubérisation »*, Paris, La Documentation française, 2017. Le règlement constitue une première réponse à l'appel au législateur lancé dans cette étude (cf. en particulier Evelyne Gebhardt, « Requêtes aux législateurs », *ibid.*, p. 161-168).

15. Cf. Philippe Escande, « Microsoft contre l'antitrust américain », *Le Monde*, 10 décembre 2022, à propos du projet de Microsoft d'acheter le studio de jeux vidéo Activision.

intermédiaires, du transport à l'hébergement, et a un champ d'application particulièrement large puisqu'il vise non seulement les fournisseurs qui ont un établissement dans l'Union mais aussi ceux qui, même établis à l'extérieur de l'Union, ont en son sein un nombre significatif de destinataires ou ciblent leurs activités sur un ou plusieurs États membres. Il est très remarquable qu'il comporte des dispositions propres aux « très grandes plateformes » et aux « très grands moteurs de recherche », définis comme ceux qui ont au moins quarante-cinq millions de destinataires actifs et désignés comme tels par la Commission européenne, ce qui vise particulièrement les GAFAM existants et à venir.

Le *DSA* comprend trois groupes de dispositions. Le premier ensemble est formé de règles qui s'appliquent à tous les services intermédiaires. Il s'agit de la définition de leur responsabilité et du régime de la lutte contre les contenus illicites. Il s'agit ensuite de différentes obligations « de diligence » qui, pour être mises en œuvre, nécessitent la création de « points de contact » tant pour les rapports avec les autorités qu'avec les destinataires de services. Au nombre de ces obligations de diligences figurent des règles détaillées sur les conditions générales des services et le régime de la modération, dont il est explicitement prévu qu'il doit respecter les droits fondamentaux. Les entreprises sont aussi tenues à des obligations de transparence, au nombre desquelles un accès des particuliers pour le signalement des contenus illicites et des règles de règlement des litiges. À noter que les contenus illicites peuvent aussi être dénoncés par des « signaleurs de confiance » reconnus comme tels par les coordinateurs nationaux des services numériques. Sont enfin précisées différentes obligations en matière de loyauté des relations commerciales et les règles de conclusion des contrats à distance.

Le deuxième ensemble, capital dans l'esprit du législateur de l'Union, concerne spécialement les « très grands » moteurs de recherche ou plateformes qui, compte tenu du nombre de leurs clients, sont désignés comme tels par décision de la Commission. Ils sont soumis à des obligations supplémentaires et renforcées : évaluation des risques systémiques et de la réaction aux crises, intervention d'audit indépendant, transparence renforcée de la publicité en ligne, accès aux données par les autorités nationales de contrôle et la Commission, création d'une fonction interne de *compliance* indépendante et publication de rapports semestriels qui portent notamment sur la modération.

Enfin, si le *DSA* prévoit que les autorités nationales de contrôle, dont l'une d'elles a la qualité de coordinateur pour les services numériques, sont en principe chargées d'assurer son respect, la Commission est

exclusivement compétente en ce qui concerne le régime spécial des très grands moteurs de recherche ou plateformes et peut aussi préempter les infractions des « très grands » aux dispositions du règlement autres que celles qui leur sont spécialement consacrées. Autrement dit, les « très grands », c'est-à-dire forcément les GAFAM, sont « la chose » de la Commission. Les coordinateurs des services numériques nationaux, autorités administratives indépendantes, sont investis de larges pouvoirs d'information, d'enquêtes et de sanction. Il appartient aux États membres d'en préciser le régime sur certains points. En particulier, le choix peut être fait de remettre la compétence en matière de sanction au coordinateur ou d'investir celui-ci du seul pouvoir de saisir la justice. En revanche, la Commission est compétente vis-à-vis des « très grands ». Les amendes peuvent aller jusqu'à
104 6 % du chiffre d'affaires mondial, les astreintes jusqu'à 1 %, et les décisions sont publiées. La Cour de justice de l'Union européenne est, comme pour le règlement « contestabilité/équité », investie d'un pouvoir de pleine juridiction.

Le statut de l'internaute

Depuis plusieurs années, la Cour de justice a développé une jurisprudence qui, anticipant parfois sur le législateur, a contribué à définir un véritable *statut de l'internaute* et, plus généralement, de l'utilisateur des NTI. Les orientations prises par la Cour sont un apport essentiel à la vision européenne du marché des NTI.

Le droit à l'oubli

J'ai qualifié de « coup de tonnerre dans le monde du Net » l'obligation faite à Google par l'arrêt *Google Spain* en 2016[16] de « déréférencer » un résultat de recherche, c'est-à-dire de l'enlever de la liste des résultats au motif qu'il porte atteinte à la vie privée. Ce *droit à l'oubli*, apport majeur de la jurisprudence de la Cour de justice, est maintenant réglementé par l'article 17 du RGPD, qui met en œuvre cette idée de bon sens que les informations de nature personnelle changent de nature avec le développement des NTI. De fugitives elles deviennent permanentes alors même qu'elles peuvent perdre pour le public tout intérêt réel mais nuire

16. C-131/12. Cf. *La Cour de justice de l'Union européenne*, *op. cit.*, p. 271 et suiv. Cf. aussi l'analyse de cet arrêt et de ses conséquences dans Francis Donnat, *Droit européen de l'internet*, Paris, LGDJ, 2018, p. 90 et suiv.

beaucoup à la personne concernée. Le droit à l'oubli joue vis-à-vis de toute entreprise qui exerce des activités dans l'Union alors même que son établissement principal serait ailleurs.

La question fort importante de la *portée territoriale* du déréférencement a été tranchée par la Cour de justice dans un arrêt du 24 septembre 2019 rendu sur un renvoi du Conseil d'État français[17]. L'obligation de suppression ne concerne pas tous les liens sur l'ensemble des versions du moteur de recherche dans le monde entier, mais seulement sur celles des États membres de l'Union. Toutefois, la Cour considère que l'Union pourrait légalement étendre cette obligation au monde entier si elle décidait de le faire[18]. En second lieu, si, dans son état actuel, le droit de l'Union n'oblige pas au déréférencement sur l'ensemble des noms de domaine, il ne l'interdit pas non plus. Il en résulte que les autorités des États membres peuvent le décider au cas par cas, compte tenu de l'appréciation qu'elles font de l'équilibre à tenir entre le droit à la vie privée et la liberté d'information.

Le « droit à l'oubli » ainsi conçu fait partie d'un droit plus général à la non-divulgation, à la « non-transparence ». Il ne s'agit pas seulement du droit de rectifier des informations fausses. Il s'agit de laisser hors de la Toile des informations exactes mais dont l'intérêt pour le public est faible alors que leur persistance dans un instrument d'accès universel peut gravement porter préjudice à l'intéressé. Ainsi la Cour a-t-elle jugé que la publication sur internet, sans aucune restriction, du montant des aides reçues par les agriculteurs dans le cadre de la politique agricole commune était excessive[19], de même qu'elle a jugé que c'est aller trop loin que de rendre accessible à tous sans restriction, sur internet, la liste des « bénéficiaires effectifs » dans le but de lutter contre le blanchiment de capitaux et le financement du terrorisme[20]. Ainsi, contrairement à ce qu'avait pu soutenir le fondateur de Facebook, la vie privée existe bien sur le Net. La Cour de justice a même posé des limites à des législations nationales en matière de corruption et de conflit d'intérêts : elle a considéré comme excessive la publication en ligne des éléments de déclaration d'intérêts de responsables publics concernant les conjoints ou partenaires, au motif que celle-ci n'était nullement indispensable pour garantir leur probité et leur impartialité[21].

17. C-507/17.
18. On peut remarquer à cet égard que l'article 17 du RGPD ne comporte aucune limitation.
19. CJCE, 9 novembre 2010, *Volker und Markus Schecke* et *Eifert*, C-92/09 et C-93/09.
20. CJUE, 22 novembre 2022, *WM* et *Sovim SA*, C-37/20 et C-601/20.
21. CJUE, 1er août 2022, *OT*, C-184/20.

La Cour de justice a aussi précisé les obligations des moteurs de recherche vis-à-vis des données dites spécifiques : origine raciale, opinions politiques ou religieuses, orientation sexuelle, données relatives aux infractions pénales. Saisi par la personne concernée, le moteur de recherche doit en principe procéder au déréférencement. Il peut toutefois s'avérer nécessaire d'apprécier sa légitimité par rapport aux impératifs de la liberté d'information, et il en va de même du compte rendu de procédures pénales. Pour ces dernières, dans le cas où le refus du déréférencement est justifié, le moteur de recherche peut être tenu d'aménager les résultats de telle manière que « l'image globale » que peut avoir l'internaute corresponde à la réalité : concrètement, si par exemple l'intéressé a été relaxé, cette information devrait apparaître en premier dans la liste des résultats[22]. Elle a confirmé l'orientation de cette jurisprudence tout
106 récemment dans un arrêt du 8 décembre 2022, *TU, RE c. Google LLC* : une personne qui fait partie de la vie publique peut demander le déréférencement de sites qui contiennent des informations fausses à son égard, ainsi que le retrait de la mise en ligne de photographies compte tenu de la valeur informative qu'elles peuvent avoir, indépendamment du contexte qui apparaît sur le site dont elles sont extraites[23].

La Cour a été amenée à se pencher sur la délicate et capitale question des *transferts de données* vers des pays tiers. Ceux-ci sont désormais réglementés par les articles 44 et suivants du RGPD. Le principe reste celui posé par la directive de 1995 : les transferts ne sont légalement possibles que si les données personnelles font l'objet dans le pays de destination d'un « niveau de protection adéquat », c'est-à-dire équivalent à celui assuré dans l'Union, ce qu'il appartient à la Commission de vérifier. Dans un arrêt qui a fait date, l'arrêt *Schrems*, du 6 octobre 2015[24], la Cour a déclaré que les conditions des transferts de données vers les États-Unis définies par la Commission en 2000 étaient incompatibles avec le droit de l'Union. L'intéressé, client de Facebook, s'était opposé à ce que ses données personnelles soient envoyées sur des serveurs aux États-Unis. La Cour de justice, saisie par la Haute Cour d'Irlande, a estimé que

22. CJUE, 19 septembre 2019, *GC et autres c. CNIL*, C-136/17. Le Conseil d'État a donné suite à cet arrêt dans une très intéressante série de décisions du 6 décembre 2019 concernant notamment la condamnation d'une femme pour violences conjugales (n° 429154), l'orientation sexuelle d'un écrivain (n° 409212), des propos tenus par un député (n° 405464) ou des atteintes aux mœurs (n° 401258). Ces décisions montrent à quel point il peut être délicat de trouver un équilibre raisonnable entre l'information et la vie privée.

23. C-460/20.

24. C-362/14 (*AJDA*, 2015, p. 2015-2263).

les règles de droit américain – contenues dans un simple document du ministère du Commerce des États-Unis qui définissait des principes généraux et comportait des réponses à des questions posées à l'administration par les entreprises, soit ce qu'on appelle de la « *soft law* » – étaient insuffisantes, et elle a confirmé ses vues à la suite de l'adoption du « bouclier de protection des données » (*privacy shield*)[25], qu'elle a encore jugé trop peu protecteur[26].

Une des caractéristiques du marché du numérique est que les opérateurs du Net cherchent par les moyens les plus divers à forcer la main des usagers ou, comme on préfère dire aujourd'hui, des clients. Le droit de l'Union lutte contre ces pratiques.

La neutralité du Net

On la qualifie de « principe fondateur » d'internet[27] ; on parle d'« internet ouvert ». La neutralité est garantie par le règlement 2015/2120[28]. Elle signifie que l'acheminement des informations doit se faire dans les mêmes conditions pour tous, sans priorité particulière, sauf si cela repose sur des exigences techniques et non pas sur des raisons commerciales.

La Cour de justice a jugé que des contrats dits de *zero rating* sont incompatibles avec le règlement[29]. En effet, ce sont des offres en vertu desquelles, lorsque le forfait est dépassé, l'utilisateur peut continuer à avoir accès à internet mais avec un débit plus lent, alors que certains services seulement sont maintenus dans les conditions antérieures. Cela aboutit à une connexion internet plus ou moins rapide selon qu'on paie plus ou moins, précisément ce que le règlement ne veut pas.

Il faut souhaiter que la Cour trouve l'occasion de consacrer la neutralité du Net comme nouvelle liberté fondamentale au titre de principe général du droit.

L'intrusion

Tous les opérateurs du numérique tentent de récupérer le maximum de données possible, notamment à des fins publicitaires. Le droit de l'Union

25. Décision 2016/1250 de la Commission du 12 juillet 2016.

26. CJUE, 16 juillet 2020, *Data Protection Commissioner c. Facebook Ireland Ltd et Maximilian Schrems*, C-311/18.

27. Cf. Garance Mathias, « La neutralité du Net, un pilier de notre démocratie », *L'Observateur de Bruxelles*, n° 126, 2021, p. 18.

28. Règlement du Parlement européen et du Conseil du 25 novembre 2015 (*JOUE*, L 310/1, 26 novembre 2015).

29. CJUE, 15 septembre 2020, *Telenor*, C-807/18 et C-39/19.

comporte des règles précises destinées à protéger le public des abus. Au nombre de ces règles, fixées notamment par la directive « vie privée et communications électroniques »[30] et le RGPD, figurent les deux principes suivants : l'équipement terminal de chacun et les informations qui y sont stockées relèvent de la vie privée ; le stockage d'informations ou la récupération d'informations qui s'y trouvent ne sont permis qu'avec le consentement de la personne concernée.

Ces deux principes sont les seuls à même de garantir la loyauté des rapports entre les opérateurs et leurs clients, dont la base doit être la liberté de choix des utilisateurs. La jurisprudence de la Cour sur les cookies en donne un bon exemple. La question lui a été posée des conditions dans lesquelles devait être donné le *consentement* à ce que des cookies soient installés. Elle a considéré qu'il n'était pas valablement
108 donné par une case cochée « par défaut », c'est-à-dire précochée, et que l'utilisateur devrait « décocher » pour refuser son consentement. C'est dans la ligne de la directive vie privée et communications électroniques qui exige un « accord », alors que le RGPD se montre encore plus exigeant : il réclame une manifestation de volonté « libre, spécifique, éclairée et univoque » qui s'exprime par « un acte positif clair » ; le droit de l'Union exige un comportement actif et non passif de la part de l'utilisateur[31].

Reste à répondre à une question capitale : peut-on valablement refuser l'accès à un site si l'utilisateur refuse les cookies ? Il appartiendra à la Cour de justice de le dire.

De même, à propos du « *like* » de Facebook, la Cour a considéré que le gestionnaire du site était responsable d'un traitement de données personnelles pour ce qui concerne leur collecte et leur transmission à Facebook. Le gestionnaire a donc l'obligation d'informer ses utilisateurs de ce que le « *like* » qui figure sur son site implique la transmission de données à Facebook et de recueillir leur accord[32].

---

30. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 (*JOUE*, L 201/37, 31 juillet 2002).

31. CJUE, 1er octobre 2019, *Planet49*, C-673/17. Le Conseil d'État français a tiré de cet arrêt de 2019 toutes ses conséquences : il a reconnu la légalité d'une sanction de 50 millions d'euros infligée par la CNIL à Google pour un manque d'informations sur les conditions d'utilisation du système d'exploitation Android et un recueil du consentement par l'utilisation d'une case précochée (CE, 19 juin 2020, *Google LLC*, n° 430810).

32. CJUE, 29 juillet 2019, *Fashion ID*, C-40/17.

*

Le monde du numérique étant en permanente évolution et les inventions quotidiennes, la Cour de justice sera forcément amenée à trancher d'autres questions essentielles pour la moralité des rapports entre les opérateurs et leurs clients : saisie de dizaines d'affaires chaque année dans ce domaine – actuellement une cinquantaine –, elle contribue de manière déterminante à la création d'une véritable philosophie de la société du XXIe siècle qui fait encore cruellement défaut.

RÉSUMÉ

L'Union européenne est sans doute une exception dans le monde d'aujourd'hui : elle affirme hautement le principe du respect de la vie privée et de la protection des données personnelles tout en essayant de construire un grand marché du numérique. Elle s'est dotée d'instruments sans équivalent ailleurs dont la Cour de justice de l'Union européenne tire toutes leurs conséquences, dans la recherche d'un équilibre délicat entre les droits fondamentaux des personnes, d'une part, et la liberté d'expression, d'information et d'entreprise, d'autre part.