La plasticité de la notion de responsable de traitement

Mélanie Clément-Fontaine

La plasticité de la notion de responsable de traitement

Mélanie Clément-Fontaine
Professeure des universités, DANTE, UVSQ, Université de Paris-Saclay.

Article publié : *Revue des Affaires Européennes*, R.A.E. – L.E.A. 2018/1, pp. 35-42.

Regulation (eu) 2016/679 of the european parliament and of the council - Controller - processor - personal or household activity - « Facebook Insights » - « Fanpage » -

Résumé - Selon une jurisprudence constante, la notion de responsable de traitement doit être interpréter de manière large afin de garantir une meilleure protection des données à caractère personnel des personnes physiques. Cela est notamment possible en raison de la plasticité de la notion de sorte qu'elle s'adapte aux activités de traitement de plus en plus complexes.

Abstract - According to settled case law, the concept of data controller must be interpreted broadly in order to guarantee better protection of natural persons with regard to the processing of personal data. This is possible in particular because of the plasticity of the notion so that it can be adapted to increasingly complex processing activities.

A l'aune de l'application du bloc européen de protection des données constitué en particulier du Règlement (UE) n° 2016/679 (RGDP)[1], l'une des grandes interrogations consiste à savoir qui échappe à la qualification de responsable de traitement tant la manipulation de données personnelles est devenue courante. En effet, la généralisation de l'exploitation des données et les moyens toujours plus nombreux d'y parvenir accroissent le risque d'identification directe ou indirecte des données à chacun de leur traitement[2]. De plus, le champ territorial d'application du régime européen de protection s'est élargi. Le RGDP s'étend à tout responsable de traitement, qu'il soit établi sur le territoire de l'Union ou pas, dès lors qu'il a recours à des moyens de traitement situés sur le territoire d'un État membre. Ainsi, il vise tout d'abord le responsable de traitement ou le sous-traitant qui dispose d'un établissement situé dans l'Union qui réalise un traitement de données à caractère personnel dans le cadre des activités de cet établissement et ce, peu importe que le traitement soit ou ne soit pas réalisé sur le territoire de l'Union[3]. Ensuite, la portée du RGDP s'étend au responsable de traitement et au sous-traitant

[1] Ce bloc est constitué du Règlement général des données personnelles (RGDP) : Règl. (UE) n° 2016/679, 27 avr. 2016) ; et de la directive : (UE) 2016/680 relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.
[2] Voir la définition de donnée personnelle énoncée à l'article 4 point 1 du RGDP.
[3] La notion d'établissement est définie dans le RGDP comme l'exercice effectif et réel d'une activité au moyen d'un dispositif stable, quelle que soit la forme juridique d'un tel dispositif. Il n'est donc pas nécessaire notamment que l'établissement soit doté de la personnalité juridique : Règl. (UE) n° 2016/679, consid. 22.

qui, bien que n'étant pas établis dans l'Union, ont des activités de traitement liées à l'offre de biens ou de services gratuits ou payants aux personnes physiques qui se trouvent sur le territoire de l'Union[4].

La qualification de responsable de traitement est d'un enjeu majeur, car elle entraîne d'importantes obligations. Aujourd'hui, le souci pour un responsable de traitement n'est plus tant de savoir s'il convient de procéder aux formalités auprès de l'autorité de régulation, celles-ci ayant été fortement diminuées[5], mais plus encore d'anticiper s'il est nécessaire de se conformer aux obligations inédites ou renouvelées prévues par l'appareil de protection. Pour mémoire, le nouveau cadre européen de protection des données personnelles emporte une profonde transformation des modalités de préservation des droits des personnes physiques. Si l'on retrouve bien entendu les obligations de transparence[6], de sécurité de l'accès aux données[7], de limitation de l'étendue et de la conservation de ces données, d'autres garanties sont venues compléter le dispositif. Il s'agit du principe de responsabilité (« accountability ») introduit par le RGDP[8] et qui se substitue au système déclaratif. Selon ce principe, un organisme responsable de traitement doit être en mesure de démontrer qu'il se conforme aux règles en matière de protection des données personnelles[9]. En pratique, il doit pouvoir établir qu'il a mis en place des mesures techniques et organisationnelles adaptées à la nature du traitement et à sa finalité. Dans le prolongement du principe de responsabilité, RGDP en consacre deux autres[10] d'origine canadienne connus sous les noms de *Privacy by design* et *Privacy by default*[11]. Il s'agit de méthodologies consistant à intégrer la protection des données personnelles dès la conception et lors de la mise en œuvre des outils de collecte, de traitement et d'exploitation des données afin de prévenir le risque d'atteinte à leur protection. Ce nouveau cadre nécessite, pour chacun, d'évaluer son rôle dans le traitement de données à caractère personnel et partant, de s'interroger sur sa qualité de responsable de traitement.

Or, il semble que la qualification de responsable de traitement tend à se généraliser pour deux raisons principales. La première tient à la définition de données personnelles qui ne cesse de s'élargir en fait et, par voie de conséquence, en droit. La notion couvre toute information se

---

[4] Règl. (UE) n° 2016/679, consid 23.
[5] Voir les nouveaux cas de formalités Règl. (UE) n° 2016/679, art. 35.
[6] Règl. (UE) n° 2016/679, art. 12 et s.
[7] Règl. (UE) n° 2016/679, art. 32 et s.
[8] Règl. (UE) n° 2016/679, art. 24.
[9] Règl. (UE) n° 2016/679, art. 24.
[10] Règl. (UE) n° 2016/679, art. 25.
[11] C. ZOLYNSKI, « Privacy by Design appliquée aux objets connectés : vers une régularisation efficiente du risque informationnel ? », *D. IP/IT* 2016, p. 404.

rapportant à une personne physique identifiée ou identifiable[12] et exclut les données anonymes. Pour autant, chacun, sans être expert en informatique, prend peu à peu conscience que la ré-identification d'une personne est à la portée de ceux qui drainent les traces numériques que nous laissons de-ci de-là parfois aussi anodines que la manière particulière de frapper les touches d'un clavier d'ordinateur[13]. La seconde raison tient à la prolifération des outils de traitement des données qui, d'un côté se démocratisent et de l'autre irrigue l'économie actuelle[14]. En effet, il est aujourd'hui commun de relever que ceux qui détiennent à la fois les plus grandes bases de données et les outils pour les valoriser occupent une place prépondérante sur le marché[15].

Partant du constat selon lequel la quasi-totalité des données fait l'objet d'un traitement et la plupart des données ont un caractère personnel, qui peut encore échapper à la qualification de responsable de traitement ? La question se pose avec d'autant plus d'acuité que l'élasticité des critères de la notion permet une large application du régime de protection des données personnelles alors que l'exception des traitements personnelle ou domestique s'entend strictement.

I. Des critères accueillants

La notion de responsable de traitement a été définie, pour la première fois, par la directive du 25 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[16] comme « *le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou tout autre*

[12] Règl. (UE) n° 2016/679, art. 4. Sur ce point, voir notamment V.-L. BENABOU, « L'extension du domaine de la donnée », dossier « Big data : quelle protection pour les données personnelles », *Legicom* n° 59, 2017/02, p. 3.
[13] Il existe une technique biométrique de reconnaissance des personnes reposant sur le rythme de frappe propre à chacun appelée « frappologie ». Elle est appliquée par exemple au mot de passe qui devient ainsi beaucoup plus difficile à reproduire.
[14] Règl. (UE) n° 2016/679, considérant 6 : « *L ' évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus, les personnes physiques rendent des informations les concernant, accessibles publiquement et à un niveau mondial. Les technologies ont transformé à la fois l'économie et les rapports sociaux, et elles devraient encore faciliter le libre flux des données à caractère personnel au sein de l'Union et leur transfert vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personne* »,
[15] M. BEHAR-TOUCHAIS (dir.), L'effectivité du droit face à la puissance des géants de l'Internet, IRIS éd. 2015.
[16] Directive 95/46/CE.

organisme qui, seul ou conjointement, détermine les finalités et les moyens du traitement de données à caractère personnel »[17].

Par ailleurs, de jurisprudence constante, la notion de responsable traitement est entendue largement afin de garantir une meilleure protection des données à caractère personnel des personnes physiques et partant de la protection de la vie privée. L'une des plus célèbres illustrations de cette jurisprudence est l'arrêt Google Spain[18]. Sans qu'il soit nécessaire de rappeler en détail cette affaire amplement commentée[19], on soulignera simplement que la Cour a adopté une conception étendue de la notion de responsable de traitement tout d'abord en retenant une appréciation généreuse de la portée territoriale de la directive 95/46[20], ensuite en considérant que l'activité de moteur de recherche doit être qualifiée de traitement de données[21] de sorte que, selon la CJUE, ce n'est pas l'utilisateur de moteur de recherche qui est responsable de traitement, mais celui qui met l'outil à disposition[22]. Enfin, la définition du responsable de traitement consacrée par le RGDP fait apparaître clairement les deux critères essentiels à savoir la capacité juridique et organisationnelle d'une part et l'autonomie à définir les finalités et les moyens du traitement d'autre part : « *est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre* ».

Les critères ainsi posés permettent d'accueillir de nouvelles pratiques dans le giron de la protection des données à caractère personnel.

---

[17] Article 2 de la directive 95/46/CE.

[18] Arrêt du 13 mai 2014, Google Spain et Google : C-131/12, EU:C:2014:317.

[19] *RTD eur.* 2014. 283, édito J.-P. JACQUE, 879, étude B. HARDY, et 2016. 249, étude O. TAMBOU ; *D.* 2014. 1476, note V.-L. BENABOU et J. ROCHFELD, 1481, note N. MARTIAL-BRAZ et J. ROCHFELD, et 2371, obs. P. TREFIGNY ; *AJDA* 2014, 1147, chron. M. AUBERT, E. BROUSSY et H. CASSAGNABERE ; *AJCT* 2014. 502, obs. O. YAMBOU ; Constitutions 2014. 218 chron. D. de BELLESCIZE ; Dossier spécial *RLDI* 2014, n° 106. C. CASTETS-RENARD, « Google et l'obligation de déréférencer les liens vers les données personnelles ou comment se faire oublier du monde numérique », *Revue Lamy droit de l'immatériel*, 2014, n° 106.

[20] F. JAULT-SESEKE et C. ZOLYNSKI, « Le règlement 2016/679/UE relatif aux données personnelles. Aspects de droit international privé » *D.* 2016 p.1874.

[21] Sur le fondement de l'article 2 b de la directive 95/46/CE, la CJUE décide que l'activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stoker temporairement et, en fin à les mettre à disposition des internautes selon un ordre de préférence donné doit être qualifié de « traitement de données à caractère personnel » lorsque ces informations contiennent des données personnelles.

[22] Voir l'application de ce raisonnement par les Cours de cassation Belge (décision du 29 avril 2016, n ° C. 15.0052 F) et française (Civ. 1, 12 mai 2016, n° 15-17.729) : notre commentaire groupé, *Auteur&Media* 2016/5-6, p. 453 et spéc. 456.

Premier critère : La capacité juridique et organisationnelle suppose que la personne (qui peut être physique ou morale, privée ou publique) agisse dans son propre intérêt, en son nom et pour son propre compte. De plus, les Etats membres ont la possibilité de désigner la personne dite responsable du traitement des données personnelles. Ainsi, selon le droit national français, la Caisse nationale d'assurance maladie (CNAMTS) qui est autorisée à procéder au traitement de données à caractère personnel relatif à la gestion et au suivi des vaccinations contre la grippe A (H1N1), est désignée par un texte réglementaire comme responsable de la création et la gestion de cette base vaccinale[23]. L'autorité de régulation de la protection des données personnelles (la CNIL), a pu en déduit que la CNAMTS est la seule responsable de traitement bien que plusieurs autres organismes interviennent dans la mise en œuvre de ce traitement. Cet exemple conduit à rappeler la distinction qui est faite entre responsable de traitement et sous-traitement. Contrairement au responsable de traitement, la mission du sous-traitant ne consiste pas à définir les finalités et les moyens de traitement, il agit pour le compte du responsable de traitement[24].

Second critère : l'autonomie à définir les finalités et les moyens du traitement permet davantage encore d'étendre la notion de responsable de traitement. Concrètement, le responsable du traitement de données à caractère personnel est la personne qui décide pourquoi et comment seront traitées ces données. Comme l'indique le groupe de travail du G29, « *la notion de responsable du traitement est une notion fonctionnelle, visant à attribuer les responsabilités aux personnes qui exercent une influence de fait, et elle s'appuie donc sur une analyse factuelle plutôt que formelle* »[25]. L'apparence simplicité du critère recèle bien des interrogations. Les situations complexes se multiplient donnant lieu le plus souvent à des responsabilités conjointes. En effet, la mise en réseau des données favorise des traitements simultanés par plusieurs acteurs de manière horizontale de sorte que chacun est susceptible d'être qualifié de responsable de traitement en lieu et place de sous-traitant. Aussi, est-il précisé notamment l'article 4 septièmement du RGDP que le responsable traitement « *est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* ». Partant, deux situations doivent être distinguées : selon la première situation, les responsables de traitement

[23] Décret n° 2009-1273 du 22 octobre 2009.
[24] Règl. (UE) n° 2016/679, art. 4.
[25] Avis 1/2010, p. 10.

déterminent ensemble les finalités et les moyens du traitement et sont alors considérés conjointement responsables[26] de sorte que la victime peut demander réparation de la totalité à l'un d'entre eux à charge, pour ce dernier, de se tourner vers son cocontractant. Dans la seconde hypothèse, ils déterminent indépendamment les finalités et les moyens du traitement alors, l'étendue de leurs obligations sera proportionnelle à leur action quand bien même le traitement porte sur les mêmes données. Le Groupe 29 résume la problématique en ces termes : *« lorsqu'il y a pluralité d'acteurs, ils peuvent entretenir une relation très proche (en partageant, par exemple, l'ensemble des finalités et des moyens d'une opération de traitement) ou, au contraire, plus distante (en ne partageant que les finalités ou les moyens, ou une partie de ceux-ci). Dès lors, un large éventail de typologies de la coresponsabilité doit être examiné, et leurs conséquences juridiques évaluées avec une certaine souplesse pour tenir compte de la complexité croissante de la réalité actuelle du traitement de données ».*

Des affaires, récentes[27], soumises à la CJUE par la voie des questions préjudicielles, illustrent la complexité de la réalité actuelle du traitement des données personnelles qui peut tenir à la fois d'une pluralité des traitements simultanés et de l'apparition de nouvelles techniques de traitement comme les codes programmes « Facebook Insights » et « le module : j'aime » d'un réseau social. En effet, ces codes programmes permettent au réseau social qui les fournit de récupérer les données personnelles des personnes visitant le site ou la page sur lesquels les programmes sont installés ; de traiter ces données aux fins de procéder à la publicité ciblée ; et de fournir au gestionnaire du site ou de la page web des statistiques sur la fréquentation. Dans ces deux affaires[28], connues respectivement sous le nom de *Fashion ID* (C-40/17) et *Fan page* (C-210/16), la CJUE doit, pour la première fois, préciser si la personne qui insère dans son site ou sa page web le code programme a la qualité de responsable de traitement. La question est épineuse dans la mesure où le réseau social détermine à titre principal les objectifs et les modalités du traitement[29], tandis que le gestionnaire du site ou de la page web est à l'origine du processus en installant le programme informatique, mais n'en a pas la maitrise. Dans

[26] Règl. (UE) n° 2016/679, art. 26 § 1.
[27] Demande de décision préjudicielle présentée par l'Oberlandesgericht Düsseldorf (Allemagne) le 26 janvier 2017 — Fashion ID GmbH & Co. KG contre Verbraucherzentrale NRW eV, JO R 112 du 10 avril 2017, (2017/C 112/32) et CJUE, Concl. avocat général Yves Bot, 24 oct. 2017, aff. C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/ Wirtschaftsakademie Schleswig-Holstein GmbH, en présence de Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht, pts 46 à 57 : *Comm. com. électr*. 2018, comm. 5, note N. METALLINOS. CJUE, aff. C210/16, 5 juin 2018, EU :C :2018 :388
[28] Préc.
[29] CNIL, Dél. n° 2017-006, 27 avril 2017, prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Irland.

l'affaire C-210/16, une société allemande, spécialisée dans le domaine de l'éducation, avait créé une « page fan » (*Fanpage*) sur le réseau social Facebook de sorte qu'elle utilise l'outil appelé « Facebook Insights ». Cet outil est proposé par Facebook gratuitement, dans le cadre de conditions d'utilisation non modifiables aux administrateurs d'une « page fan ». Il permet à ces derniers d'obtenir des statistiques anonymes élaborées par Facebook à partir des données personnelles des personnes qui consultent la page et selon des critères qui peuvent être personnalisés par l'administrateur. Par ailleurs, Facebook utilise ces données personnelles afin de diffuser de la publicité ciblée. L'autorité régionale de protection des données de Scheswig-Holstein (l'ULD) avait, par décision du 3 novembre 2011, ordonné à l'administrateur de désactiver la page fan qu'il avait créée sur Facebook sous peine d'astreinte au motif que ni lui ni Facebook n'informaient les visiteurs de la page que ce dernier collectait leurs données à caractère personnel et qu'il les traitait. L'administrateur a alors introduit une réclamation contre cette décision dans laquelle il faisait valoir qu'il n'était ni responsable du traitement des données effectué par la société Facebook ni des cookies installés par elle. Par décision du 16 décembre 2011, l'UDL a rejeté cette réclamation considérant qu'en créant la page fan l'entreprise apportait également une contribution active et volontaire à la collecte de données à caractère personnel par Facebook, dont elle profitait grâce à des statistiques concernant les utilisateurs mis à disposition par ce réseau. L'entreprise a alors introduit un recours à l'encontre de cette décision devant le tribunal administratif allemand en faisant valoir notamment que l'ULD s'est retournée à tort contre elle et non directement contre Facebook. Le tribunal administratif, par un arrêt du 9 octobre 2013, lui donna raison en jugeant qu'elle n'était pas « organisme responsable » au sens de l'article 3 paragraphe 7[30] de la loi fédérale sur la protection des données et par conséquent annula la décision de l'ULD. La décision ayant été confirmée par le tribunal administratif supérieur allemand, l'ULD forma un recours en *Révision* devant la Cour administrative fédérale. Il est intéressant de s'arrêter un instant sur les motifs conduisant la Cour à ne pas qualifier la société administratrice de la page de responsable de traitement. La Cour considère que l'intimé ne détermine pas les finalités et les moyens de traitement de données personnel dans la mesure où, en prenant la décision de recourir à l'outil mis à disposition par Facebook, il n'a pas la possibilité d'influencer, de guider, de modeler ou encore de contrôler la nature et l'étendue du traitement des données des utilisateurs de sa page fan par Facebook en raison de l'absence de négociation des conditions d'utilisation fixées unilatéralement par Facebook ni encore lui interdire de collecter et de traiter ces données. Par

[30] Qui dispose que « *on entend par organisme responsable toute personne ou tout organisme qui collecte, traite, ou utilise des données à caractère personnel, pour son compte ou par l'intermédiaire d'autrui en sous traitance* ».

ailleurs, elle relève que le profit tiré de l'outil (l'obtention des statistiques de données anonymes) par l'administrateur n'est pas suffisant pour la qualifier de responsable de traitement. Partant de ce postulat, la Cour décida de sursoir à statuer pour demander entre autres à la CJUE, si l'ULD était fondée à exercer ses pouvoirs d'intervention à l'encontre d'une personne n'ayant pas la qualité de traitement au sens de l'article 2, sous d), de la directive 95/46, mais qui pourrait malgré tout être tenue responsable en cas d'atteinte aux règles relatives à la protection des données à caractère personnel du fait de recourir à un réseau social tel que Facebook pour diffuser son offre d'informations. Or l'avocat général[31] conteste le postulat de la Cour selon lequel l'administrateur n'est pas responsable de traitement et considère, au contraire, qu'il est responsable conjointement avec Facebook de la phase du traitement consistant dans la collecte de données à caractère personnel[32]. La raison principale avancée par l'avocat général tient au fait que l'administrateur exerce une influence déterminante sur le déclenchement du traitement des données à caractère personnel des personnes qui consultent sa page et inversement, il dispose du pouvoir de faire cesser ce traitement en fermant sa page fan. Par ailleurs, en ciblant un certain public il oriente les catégories des personnes dont les données seront collectées par Facebook. De plus, pour l'avocat général les responsables conjoints de traitement poursuivent des finalités étroitement liées : l'administrateur veut améliorer sa communication grâce aux statistiques d'audience et Facebook veut mieux cibler la publicité diffusée sur son réseau. Enfin, retenant une appréciation *in concreto* à partir des faits de l'espèce, l'avocat général rejette l'interprétation de la Cour tirée d'après lui exclusivement des clauses et des conditions du contrat conclu entre les protagonistes. Il rappelle à ce titre « *il n'est pas nécessaire pour être qualifié de responsable de traitement au sens de la directive 95/46 de disposer d'un pouvoir de contrôle sur tous les aspects du traitement. Affirmer le contraire, conduirait à limiter sérieusement la protection des données personnelles compte tenu de la complexité actuelle des traitements faisant intervenir plusieurs acteurs aux rôles complémentaires. Enfin, dans un souci de garantir la protection des personnes physiques, il importe de ne pas ouvrir une brèche qui consisterait à échapper aux obligations de responsable de traitement dès lors que l'on a recours aux services d'un tiers. Une interprétation contraire créerait un risque de contournement des règles relatives à la protection des données à caractère personnel* »[33]. L'avocat général poursuit son analyse en ce référent à une autre affaire qui n'a pas encore été tranchée par la Cour (C-40-17). Dans cette dernière affaire dite *Fashion*

[31] Conclusions de l'avocat général M. Yves Bot, présentées le 24 octobre 2017, UE :C :2017 :796.
[32] Affaire C-210/16, Concl. point 42.
[33] Affaire C-210/16, Concl. point 65.

ID, le gestionnaire d'un site web, la société Fashion ID a inséré dans son site ce que l'on appelle un « module social » (en l'occurrence le bouton « j'aime » de Facebook) d'un fournisseur externe (c'est-à-dire Facebook), qui entraîne une transmission de données à caractère personnel de l'ordinateur de l'utilisateur du site web au fournisseur externe. Une association de protection des consommateurs reproche à la société Fashion ID d'avoir ainsi permis à Facebook l'accès aux données à caractère personnel des utilisateurs de ce site, sans leur consentement et ce, en violation des obligations d'informations. La question posée à la CJUE consiste à déterminer si la Société Fashion ID est un responsable de traitement. Pour l'avocat général, les faits sont comparables à l'affaire *Fan page* (C-210/16) et conduisent à la même conclusion : l'administrateur d'une page ou l'exploitant d'un site web qui intègre le code d'un fournisseur de services de webtracking à son site web contribue à la transmission de données personnelles, l'installation de cookies et la collecte de données au profit du fournisseur de services de webtracking en sus du leur. Le gestionnaire d'un site web qui utilise ces modules sociaux est ainsi également un responsable de traitement au sens de la Directive 95/46 (et du RGPD). La CJUE, par son arrêt rendu le 5 juin 2018, reprend en substance les conclusions de l'avocat général[34].

Si l'on poursuit le raisonnement de l'avocat général, rien n'interdit de qualifier les utilisateurs d'un réseau social de responsables de traitement sauf à considérer que cette activité est strictement personnelle et domestique. L'arrêt rendu par la CJUE ne permet pas totalement de lever le doute. En effet, bien que la Cour précise que « *si le simple fait d'utiliser un réseau social tel que Facebook ne rend pas l'utilisateur de Facebook coresponsable d'un traitement de données à caractère personnel effectué par ce réseau* »[35], elle procède à une appréciation *in concreto*. Aussi, hormis le cas exceptionnel de traitement dans le cadre d'activités strictement personnelles ou domestiques, rien ne justifie que la coresponsabilité ne soit reconnue dès lors qu'il y a un traitement de données personnelles effectué à l'aide des outils fournis par un réseau social.

II. L'exclusion des activités strictement personnelles ou domestiques

Selon le considérant 18 du RGDP, n'entrent pas dans le champ de protection les traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques. Le texte vise en particulier l'échange de

[34] Précitées, points 25 à 44.
[35] CJUE, 5 juin 2018, précitée, point 35.

correspondance et la tenue d'un carnet d'adresses, l'utilisation de réseaux sociaux et, enfin, les activités en ligne qui ont lieu dans le cadre de ces activités.

A titre liminaire, trois observations d'ordre général sur la portée de l'exception doivent être faites : tout d'abord, l'exception ne se borne pas aux seuls cas d'activités personnelles ou domestiques énumérés dans le texte. Par conséquent, le caractère non limitatif de la liste permet d'envisager d'autres activités susceptibles d'être personnelles ou domestiques ; ensuite, la liste ne lie pas le juge qui apprécie *in concreto* la situation afin de déterminer s'il s'agit réellement d'une activité personnelle ou domestique ; enfin, l'exception ne bénéficie pas aux responsables de traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques.

A ce stade, s'il demeure hasardeux de cartographier de manière abstraite ce qui relève effectivement d'une activité personnelle ou domestique et partant d'anticiper l'interprétation qu'en feront les juges, les exemples cités dans le considérant 18 du RGDP appellent une première série de réflexions.

Le premier exemple, relatif à l'échange de correspondance et la tenue d'un carnet d'adresses, est sans doute celui qui pose le moins de difficultés. L'exclusion du champ de la protection des données personnelles des carnets d'adresses personnels est déjà connue. En effet, elle est notamment consacrée à l'article 2 de la loi de 1978. Quant à la correspondance privée, elle a fait l'objet d'une importante jurisprudence tendant à tracer la frontière d'avec la correspondance professionnelle.

Le deuxième exemple, qui vise l'utilisation de réseaux sociaux, est sans doute davantage délicat à apprécier. Si l'on suit les conclusions de l'avocat général dans l'affaire *Fan page* (C-210/16), celui qui a recours aux outils d'un réseau social permettant à ce dernier de traiter des données personnelles peut être qualifié conjointement de responsable de traitement. Certes, la solution préconisée par l'avocat général était guidée par le fait que l'affaire concernait clairement l'activité professionnelle d'une entreprise. De plus, la CJUE a pris soin de préciser que la simple utilisation d'un réseau social ne rend pas l'utilisateur coresponsable de traitement. Pour autant, *a contrario*, il est raisonnable d'en déduire que si l'usage du réseau social est réalisé par une personne physique et est strictement personnel alors il ne relève pas du champ de protection des données à caractère personnel. Mais entre l'usage professionnel et l'usage personnel bien des variantes sont possibles. L'expérience montre, en effet, que l'utilisation des réseaux sociaux est souvent à la fois personnelle et professionnelle. Par exemple, si l'on peut considérer que Linkedln est un réseau principalement professionnel, en revanche Facebook n'est ni un réseau à dominante professionnelle ni un réseau à dominante personnelle ou domestique : le même

compte utilisateur est parfois utilisé indifféremment pour l'une ou l'autre de ces finalités. En ce cas, suivant une interprétation large du champ d'application de la protection des données personnelles retenue par les juges, l'activité professionnelle bien que marginale devrait conduire à soumettre l'usage du réseau social au RGDP. Une telle interprétation est renforcée par la formule consacrée selon laquelle seules les activités *strictement* personnelles ou domestiques sont concernées par la limitation.

Le troisième exemple vise les activités en ligne qui ont lieu dans le cadre de ces activités au rang desquelles il semble que l'on puisse retenir les sites personnels mentionnés à l'article 2 de la loi 1978. Ce dernier exemple renforce la thèse selon laquelle, les cas énoncés par le considérant 18 ne sont pas limitatifs et permettront l'adaptation du texte aux évolutions technique et sociale des outils numériques. Ainsi, un des problèmes actuels est de savoir si le *Cloud personnel* correspond à une activité personnelle ou domestique et s'il relève de l'exception prévue au considérant 18 du RGPD. En substance, le *Cloud personnel* est un serveur sécurisé de stockage des données d'une personne dont elle a l'exclusivité de l'accès. Les sociétés qui offrent de telles solutions aux individus espèrent de la sorte échapper aux obligations incombant à un responsable de traitement dans la mesure où elles n'ont ni accès aux données ainsi stockées ni le pouvoir d'en contrôler le traitement. Pour autant, ces sociétés fournissent les moyens de traitement à défaut d'en concevoir les finalités. A ce titre, elles pourraient être qualifiées de responsables de traitement. Quant à l'utilisateur de *Cloud personnel*, rien ne s'oppose à ce qu'il endosse également la qualité de responsable dès lors que l'usage n'est pas strictement personnel ou domestique, et que les données qu'il traite sont les données personnelles de tiers. Cette solution technique destinée à permettre aux personnes de maitriser la confidentialité de leurs données personnelles pourrait finalement entrer dans le champ d'application de la protection des données à caractère personnel.

***

En conclusion, la raison de l'extension du nombre de personnes éligibles à la qualité de responsable de traitement ne nous semble pas résulter d'une dérive protectionniste du législateur ou encore du juge. Elle tient, en vérité, à la généralisation des traitements de données personnelles qui se banalisent. Le phénomène révèle la vulnérabilité de la protection de la vie privée au sein d'une société dans laquelle, inexorablement, les données identifiées ou identifiables sont égrainées. Inversement, la plasticité de la notion de responsable de traitement permet son adaptation aux nouvelles pratiques qui se complexifient. La CJUE a ainsi apporté

trois éclairages déterminants : premièrement, le RGDP s'applique aux traitements mixtes, c'est-à-dire dont la finalité est à la fois personnelle et professionnelle ; deuxièmement, est responsable de traitement celui qui définit les finalités et/ou les moyens de traitement *même partiellement* ; enfin, troisièmement la CJUE souligne « *l'existence d'une responsabilité conjointe ne se traduit pas nécessairement par une responsabilité équivalente des différents opérateurs concernés par un traitement de données à caractère personnel. Au contraire, ces opérateurs peuvent être impliqués à différents stades de ce traitement et selon différents degrés, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances du cas d'espèce* »[36].

La prochaine étape consistera à trancher le sort des traitements d'ensembles mixtes de données — à savoir personnelles et non personnelles — qui constituent une grande partie des données traitées. La réponse résultera de l'articulation retenue entre le futur Règlement relatif à la libre circulation des données[37] et le RGDP[38]. En particulier, il s'agira de préciser quel texte s'appliquera lorsque les données d'un ensemble mixte sont inextricablement liées c'est-à-dire qu'elles ne peuvent être techniquement dissociées de sorte qu'une application distributive des régimes n'est pas envisageable. L'enjeu est de taille pour les entreprises qui souhaitent échapper à la qualification de responsable de traitement[39]. Il ne semble pas que l'on s'achemine vers une solution tranchée[40] malgré quelques voix en ce sens[41]. Le risque est de créer de nouvelles incertitudes quant à savoir qui est responsable de traitement.

---

[36] CJUE du 5 juin 2018 pré., point 43.

[37] Proposition de Règlement du parlement européen et du conseil concernant un cadre applicable à la libre circulation des données non personnelles dans l'Union européenne du 13 septembre 2017 COM (2017) 496 final.

[38] Voir sur ce point, par exemple, la proposition de résolution n° 80 (2017-2018) de M. Sutour déposée au Sénat le 9 novembre 2017, ainsi que la Résolution n° 24 (2017-2018), devenue résolution du Sénat le 5 décembre 2017.

[39] Pour une solution favorable aux entreprises, voir l'amendement n° 5 relatif au considérant 10 du Projet d'avis du 30 janvier 2018, 2017/0228 (COD). PE613.537v01-00 (rapporteur Zdzislaw Krasnodebski) selon lequel le RGDP s'applique « *à moins que les données à caractère personnel ne figurent dans l'ensemble de données qu'à des fins administratives et ne soient pas des données à caractère sensibles* »

[40] Projet de rapport 2017/0228 (COD). PE-619.038v01-00 et Projet de rapport du 9 avril 2018 : 2017/0228 (COD). PE-619.414v02-00 (rapporteur Anna Maria Corazza Bildt) : « lorsque *des données à caractère non personnel et personnel d'un ensemble de données mixtes sont inextricablement liées, le présent règlement devrait s'appliquer à tout l'ensemble sans préjudice du règlement (UE) 2016/679 ».*

[41] Voir les amendements 70 à 79. Par exemple l'amendement 79 présenté par Julia Reda au nom du groupe Verts/ALE visant à qualifier les ensembles de données « mixtes » de données personnelles en vue de l'application du RGDP. Pour une application du Règlement sur la libre circulation des données aux ensembles de données mixtes : amendements 80, 81. Pour la suppression du considérant 10 : amendement 69.