

# Données personnelles : quels nouveaux droits ?



Entretien avec

Judith ROCHFELD

Professeure à l'École de droit de la Sorbonne, directrice du Master 2 « Droit du commerce électronique et de l'économie numérique », co-directrice de l'Institut de recherche juridique de la Sorbonne<sup>1</sup>

Statistique et société a présenté dans son numéro d'automne de 2016 les principales dispositions de la loi « Pour une République numérique » concernant les *données publiques* (titre I de la loi). La question des *données personnelles* est au moins d'égale importance. Elle concerne tous les utilisateurs de services informatiques en ligne, c'est-à-dire tout le monde ; elle concerne aussi particulièrement les producteurs et les utilisateurs de travaux statistiques, car ceux-ci ont de plus en plus affaire à des données sur des personnes, et doivent respecter dans leur pratique professionnelle le droit en vigueur. Le titre II de la loi République numérique est consacré à cette question, qui vient également de faire l'objet d'un règlement européen. Celui-ci va se substituer à la plupart des dispositions de la loi Informatique et Libertés que la France connaît depuis 1978. Nous avons demandé à Judith Rochfeld, spécialiste du droit de l'économie numérique, d'éclairer nos lecteurs sur les nouveautés contenues dans ces deux textes.

**Statistique et société** : La loi « Pour une République numérique »<sup>2</sup> promulguée en octobre 2016 contient des dispositions sur « la protection des droits » dans son titre II. Cette même année, l'Union Européenne a adopté le règlement 2016/679 « Protection des personnes physiques à l'égard du traitement des données à caractère personnel ». Comment ces deux textes s'articulent-ils ? Qu'est-ce qui va rester original dans le droit français ?

**Judith Rochfeld** : Le texte européen sera applicable partout dans l'UE le 25 mai 2018 : à partir de ce moment, conformément aux principes généraux du droit, ce texte, dans son champ d'application, se substituera aux lois nationales<sup>3</sup>, et sera le seul texte applicable. Une discussion reste possible sur des questions qui seraient à la frontière du champ d'application de ce règlement. Par exemple, la loi française pour une république numérique contient des dispositions sur « la mort numérique » différentes de celles qui figurent dans le règlement européen. Si l'on considère que ce sujet était dans le champ couvert par le règlement européen,

1. Judith Rochfeld est l'auteur de nombreux livres et articles, parmi lesquels *A qui profite le clic ? Le partage de la valeur à l'ère numérique*, co-écrit avec Valérie-Laure Bénabou - O. Jacob, 2015 ; et *Le projet de loi pour une République numérique : entre espoirs et regrets - Dalloz IP/IT* n°1 janvier 2016

2. Loi 2016-1321 du 7 octobre 2016

3. Notamment plusieurs articles de la loi « Informatique et Libertés » de 1978. Cela dit, de nombreuses dispositions de la loi Informatique et libertés resteront en vigueur : par exemple, toutes celles qui portent sur le rôle et l'organisation de la Commission nationale de l'informatique et des libertés (Cnil).

les dispositions de la loi française cesseront en 2018 d'avoir force juridique. Mais on peut aussi considérer que c'est un sujet qui relève du droit des successions, et se trouve donc en dehors de la compétence européenne : auquel cas la loi française restera applicable.

Par ailleurs, ce règlement a la particularité de comporter beaucoup d'options constituant des marges de manœuvre nationales. C'est le cas en ce qui concerne les éventuelles « actions collectives » pour faire respecter le droit à la protection des données personnelles. De telles actions pourraient par exemple être intentées par des individus touchés par une faille de sécurité du système informatique d'une entreprise dont ils sont clients (en l'état du droit actuel, cette action est possible pour obtenir la cessation d'un manquement à la loi du 6 janvier 1978). Le règlement européen évoque cette possibilité, mais ne va pas plus loin : il appartiendra aux lois nationales de préciser la portée de cette disposition.

**S&S** : Est-ce que la loi nationale pourrait aller au-delà du règlement européen, être plus protectrice ?

**JR** : Attention ! Rappelez-vous le titre complet du règlement européen : c'est un règlement 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* ». Le deuxième membre de phrase ne doit pas être oublié : le règlement n'est pas seulement un outil de protection des personnes, c'est aussi un instrument de régulation dans le sens du marché unique. Si une loi nationale protégeait davantage que le règlement, elle créerait une distorsion de marché, en défavorisant les entreprises qui y seraient soumises par rapport aux autres. Par exemple, témoignage de cette protection des utilisations des données, les « intérêts légitimes des responsables de traitements » sont reconnus, par ce règlement comme par la directive qui le précédait, comme une cause légitime de traitement des données des usagers (d'une plateforme par exemple).

**S&S** : Que recouvre cette expression « intérêts légitimes des responsables de traitements » ?

**JR** : C'est un des six fondements qui peuvent rendre légitime un traitement de données personnelles. Ces fondements sont : 1° Le consentement des personnes concernées ; 2° La nécessité pour l'exécution du contrat auquel la personne concernée est partie ; 3° La nécessité pour le respect d'une obligation légale à laquelle le responsable du traitement est soumis ; 4° la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ; 5° La nécessité pour l'exécution d'une mission d'intérêt service public ; 6° La nécessité du traitement pour les intérêts légitimes du responsable du traitement (en balance avec les droits fondamentaux de la personne concernée par le traitement). D'après ce dernier motif et selon l'interprétation qui en est faite, un opérateur pourrait invoquer son modèle économique pour justifier de traiter des données personnelles. Dans quelle mesure cette invocation est-elle acceptable ? C'est typiquement une question d'interprétation, susceptible d'être différente selon les pays, et arbitral en dernier ressort par la Cour de Justice de l'UE.

**S&S** : La définition de ce qu'on considère comme des « données à caractère personnel »<sup>4</sup> dans le champ juridique a-t-elle évolué avec ces nouveaux textes ? Toutes les données fournies par une personne physique à des fournisseurs de services informatiques sont-elles des données à caractère personnel au sens juridique ?

**JR** : Dès lors qu'une donnée est liée à une personne identifiée ou identifiable, elle est considérée comme « personnelle » en droit européen : « porter une cravate grise » peut être

---

4. « Données à caractère personnel » est le terme exact, retenu aussi bien dans la loi française que dans le règlement européen. Dans le langage courant, on utilise plus souvent « Données personnelles ».

une donnée à caractère personnel... Cette définition, bien stabilisée désormais, est considérée comme très large par les Américains. L'une des nouveautés du texte européen est de parler, à l'inverse, de « donnée anonyme » lorsque tout lien avec la personne a été rompu, si tant est que cela soit possible, et de « donnée pseudonymisée »<sup>5</sup>. Cela dit, les données personnelles ne sont pas toujours « fournies » par les personnes concernées : elles peuvent aussi être captées à l'insu de ces personnes, notamment lorsqu'une telle captation est la contrepartie tacite de services gratuits. La définition juridique de ce qui est « collecte » et de ce qui est « traitement » de données personnelles est suffisamment large pour inclure ces cas.

La petite divergence qui existait entre les définitions de la directive européenne et de la loi française à propos de ce qu'est une donnée à caractère personnel subsiste : une information qui nécessiterait, pour identifier la personne à laquelle elle se rapporte, la mise en œuvre de moyens « déraisonnables » n'est pas considérée comme une donnée à caractère personnel par le règlement européen, mais elle l'est, selon la loi française. La référence au caractère « raisonnable » des moyens à mettre en œuvre ne figure pas dans le texte lui-même du règlement, mais dans ses « considérants ». Il est à noter que la Cour européenne de Justice se réfère parfois à ces « considérants ».

**S&S** : Quels sont les droits nouveaux dont disposent les individus par rapport à leurs données personnelles ?

**JR** : Rappelons d'abord les droits déjà formulés antérieurement : droit des personnes à être informées sur l'existence d'un traitement de données personnelles la concernant, d'y accéder, de les faire corriger si elles sont inexactes, de les faire supprimer si la durée de conservation correspondant à la finalité du recueil est dépassée. Tous ces droits figuraient déjà dans la directive européenne de 1995 et dans la loi Informatique et Libertés en France. Deux autres droits sont apparus dans la jurisprudence de la Cour de justice de l'Union Européenne, et sont inscrits dans le nouveau règlement : le droit à la portabilité de ses données et le droit au déréférencement.

**S&S** : Portabilité, comme pour le numéro de téléphone lorsqu'on change d'opérateur téléphonique ?

**JR** : Non, pas exactement. Dans le cas du numéro de téléphone, il s'agissait, dans un esprit de respect de la concurrence, de protéger les droits économiques des consommateurs qui risquaient d'être prisonniers de leurs opérateurs. Dans le cas des données personnelles, il s'agit surtout d'appliquer un autre principe, désormais inscrit dans l'article premier de la loi Informatique et Libertés, selon lequel « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant », autrement appelé le principe « d'autodétermination informationnelle »<sup>6</sup>. Selon ce principe, qui instaure une nouvelle conception du rapport de la personne avec ses données, chaque individu se voit reconnaître une certaine autonomie dans la gestion de ses données personnelles. En particulier, s'il souhaite changer d'opérateur pour un service particulier, il doit pouvoir emporter avec lui les données personnelles qu'il avait constituées avec son ancien opérateur<sup>7</sup>. L'application de ce

---

5. Article 4, 5° du règlement européen : la pseudonymisation fait que les données ne peuvent plus être attribuées à une personne concernée précise « sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ». Par exemple, il ne suffit pas de remplacer les identifiants personnels – nom, prénom, ou numéro d'inscription au répertoire national d'identification des personnes physiques – par des numéros sans signification pour obtenir un fichier « pseudonymisé » ; encore faut-il qu'aucune combinaison des variables présentes dans le fichier ne permette une identification d'un individu. De telles variables, si elles existent, doivent être conservées séparément, dans un fichier distinct du fichier « pseudonymisé ».

6. Notamment par la Cour constitutionnelle allemande et par le Conseil d'État français.

7. Par exemple, sa propre liste de morceaux de musique préférés.

droit nécessite évidemment que les données en question puissent être séparées des données d'autres personnes, ce qui n'est pas toujours facile, ni même concevable, dans un contexte où les interactions entre utilisateurs d'un service sont intenses, et souvent constitutives de la valeur des données (commentaires, notations, etc.).

**S&S :** Et le droit au déréférencement ? S'agit-il d'un « droit à l'oubli » sur Internet ?

**JR :** Certains l'appellent ainsi, mais c'est abusif. Une personne qui s'estime lésée parce qu'une information la concernant est systématiquement associée à une recherche par son nom sur un moteur de recherche peut obtenir que cette information soit « déréférencée » par ce moteur ; mais pas qu'elle soit effacée des sites Internet où elle figure. En quelque sorte, il s'agit de diminuer la visibilité d'une information, non de la supprimer. Ce droit, qui a émergé en 2014 lors d'un arrêt célèbre de la Cour de justice de l'UE<sup>8</sup>, a en partie été inscrit dans le nouveau règlement européen. La discussion autour de ce droit reste néanmoins intense : son application peut entrer en conflit avec la liberté d'expression, et fait naître le risque que la mémoire collective soit « subjectivée » par les désirs individuels (que l'on efface une information parce qu'elle est gênante pour un individu)<sup>9</sup>. Des exceptions sont d'ailleurs prévues pour la défense des libertés d'expression et d'information ainsi que pour les besoins des archives, et du travail journalistique ou scientifique ; des critères d'articulation s'élaborent. À cet égard, se pose la question : « qui doit arbitrer ? ». Actuellement, c'est Google qui reçoit des particuliers les demandes de déréférencement et décide, ou non, d'y donner suite : cela revient à donner à un opérateur privé un rôle d'arbitre entre des libertés fondamentales. Ce droit, qui pouvait déjà être extrapolé en France à partir de la loi de 1978 dans une version plus limitée<sup>10</sup>, a été « poussé » par la décision de la Cour de justice de l'UE, et cette version plus forte a été confirmée, avec des nuances, dans le règlement européen. En pratique, pour l'instant, il s'applique principalement à l'égard des moteurs de recherche, moins des éditeurs de contenus.

**S&S :** N'y a-t-il pas une disposition spécifique sur le déréférencement pour les mineurs dans la loi République numérique ?

**JR :** Vous avez raison : cette loi française prévoit un « droit au déréférencement » pour les mineurs. De façon générale, parmi les critères permettant de juger de l'opportunité d'un déréférencement<sup>11</sup>, la sensibilité des données révélées pour les personnes concernées figure en bonne place, à côté du caractère public ou non public de la personne et de l'importance de l'information en question pour le débat général. Pour un mineur, cette sensibilité est forte : le risque d'un préjudice important quant à la vie privée pèse pour eux plus lourd que les autres critères. D'ailleurs aux États-Unis, où il n'existe guère de lois de protection générale en matière de données personnelles, la Californie a instauré un droit de ce genre pour les mineurs.

**S&S :** La finalité des traitements joue un rôle important dans la loi de 1978 : avant de collecter des données personnelles auprès de quelqu'un, tout opérateur doit l'informer du « pourquoi » de cette collecte, et il doit exister une proportionnalité entre les données collectées et le but poursuivi. Est-ce toujours le cas, à l'heure où les données sont souvent collectées de façon invisible pour l'utilisateur d'un service ou d'une application ?

**JR :** Oui, c'est toujours le cas. Lorsqu'on vous avertit que des « cookies » vont être installés

---

8. Arrêt « Google Spain » qui a imposé à la filiale espagnole de Google de déréférencer une information concernant le passé judiciaire d'un citoyen espagnol

9. Vallespi E. et Wales J. (2016) « Le « droit à l'oubli » ne doit pas tourner à la censure » *Le Monde* 26 novembre 2016

10. Lorsque la durée de conservation d'une information apparaissait comme disproportionnée au regard de la finalité du traitement, la personne concernée par cette information pouvait déjà demander qu'elle soit effacée.

11. Critères mis au point entre le « groupe des autorités européennes » (CNIL et ses équivalentes dans les autres pays) et Google après l'arrêt de 2014

sur votre ordinateur, on vous explique que c'est nécessaire pour assurer le service dont vous désirez bénéficier, voire pour l'améliorer. Le fournisseur se met ainsi en conformité avec la loi qui exige de lui d'être transparent sur la finalité de la collecte et sur l'usage qui sera fait des données.

**S&S** : Est-ce que les droits des individus par rapport à leurs données personnelles ne seraient pas mieux protégés si ces données étaient considérées comme leur propriété, comme faisant partie de leur patrimoine ? N'est-on pas « propriétaire de ses données » ?

**JR** : C'est une question très importante. La réponse du législateur européen et français est négative : selon lui, la notion « d'autonomie informationnelle » (voir plus haut) est susceptible d'assurer une meilleure protection que la notion de propriété. Et je suis de cet avis. Mais cela mérite une explication détaillée.

Lors des débats internationaux sur ce sujet, l'option « propriété » a été soutenue de plusieurs côtés. Les opérateurs américains, publics et privés<sup>12</sup>, ont soutenu être propriétaires des données qu'ils traitent, apurent, enrichissent... Et du côté des défenseurs des droits des personnes, certains estimaient et estiment toujours que la meilleure protection consiste à se prévaloir d'un droit de propriété de chacun sur ses données, permettant d'en réclamer la valeur et d'être associés aux bénéfices de leur utilisation. Pour ces personnes, le rapport aux données est de l'ordre de « l'avoir ».

L'autre option, qui l'a finalement emporté au niveau européen, considère les données personnelles comme liées à « l'être » lui-même, à son identité, dont elles constituent un « reflet numérique ». Et chaque personne doit pouvoir décider comment elle se rend visible par ses données : c'est le fondement du concept d'autonomie informationnelle. Dans cette conception, les données personnelles ne relèvent pas du droit patrimonial, mais du droit de la personne (de la vie privée, de la non-discrimination, etc.). D'ailleurs, les risques principaux que la personne encourt du fait de ses données sont-ils des risques de perte de valeur ? Non, car la valorisation des données d'une seule personne ne représente presque rien, « epsilon » dans un ensemble où c'est la masse globale des données et des liens entre elles qui peut faire l'objet d'une valorisation économique. Les risques réels ne sont pas là : ils concernent les libertés fondamentales des personnes, qui peuvent faire l'objet, sur le fondement de ces données personnelles, de profilages, de discriminations<sup>13</sup>, de révélations de leur vie privée, de harcèlement, etc. Toutes choses qui sont plus de l'ordre de « l'être » que de « l'avoir ». La « charte des droits fondamentaux » de l'Union Européenne, dans son article 8, protège d'ailleurs les données comme un droit fondamental, dissocié de la vie privée, mais lié à la personne.

Dès 2014, le Conseil d'État français s'était également prononcé dans ce sens, en soulignant que la protection des données par leur valeur économique individuelle risquait d'être inopérante<sup>14</sup>.

Mais le débat reste ouvert au niveau mondial.

**S&S** : Qu'en est-il dans ces conditions de la « mort numérique » ? Que deviennent nos droits sur nos données personnelles à notre mort ?

**JR** : La loi République numérique contient à ce sujet une disposition qui s'inscrit bien dans le principe d'autonomie informationnelle : elle prévoit la possibilité pour une personne de

---

12. Pour faire image : « Obama et la Silicon Valley » !

13. À l'embauche, ou pour l'attribution de prêts, d'assurances...

14. Étude 2014 du Conseil d'État sur le numérique et les droits fondamentaux – disponible sur le site <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf>

désigner quelqu'un pour décider du sort de ses données personnelles après sa mort. Mais la question du traitement successoral de cet ensemble de données reste ouverte et l'on peut également voir là la reconnaissance des données comme « patrimoine » (« avoir », donc).

**S&S :** On comprend bien ce principe d'autonomie informationnelle, on peut y adhérer, mais est-il susceptible de passer réellement dans les faits ? Comment le rendre effectif ?

**JR :** La première affirmation de ce principe remonte à 1983, et a été faite par la Cour Constitutionnelle d'Allemagne fédérale à propos du recensement de la population !<sup>15</sup> S'agissant de son effectivité, je crois qu'il faut considérer ce principe comme un « chapeau » pour les droits plus précis déclinés en vertu de lui : droit d'être informé sur les finalités, droit d'accès, de déréférencement, etc. C'est chacun de ces droits particuliers qui doit être rendu effectif, pour donner force au principe général.

**S&S :** Il n'y a pas que le sort de leurs données personnelles qui peut préoccuper les individus, il y a aussi la question des algorithmes. Les algorithmes prennent des décisions, ou contribuent à des décisions qui influent sur la vie de tous. Faut-il nous protéger contre les algorithmes ? Est-ce que le droit s'est emparé de cette question ?

**JR :** Cette préoccupation ne date pas d'hier, et la loi de 1978 prévoyait déjà qu'aucune décision affectant une personne ne devait être prise uniquement sur la base d'un traitement automatisé. La loi pour une République numérique a, un moment, eu pour ambition, au titre de l'exigence de « loyauté des plateformes »<sup>16</sup>, que celles-ci rendent transparents pour l'utilisateur les modes de traitements des données de ces derniers. Néanmoins, cette « transparence » n'a finalement été imposée que dans les relations entre les administrations publiques et les usagers : l'article 4 de cette loi introduit une obligation pour l'administration, d'expliquer les critères mis en œuvre par l'algorithme pour prendre une décision à l'égard de l'utilisateur si ce dernier en fait la demande (une mention doit le prévenir qu'un algorithme est intervenu). À ce propos, le contentieux de l'application « Admission post-bac » (APB) va être très intéressant à observer : de nombreux parents contestent les affectations proposées à leurs enfants et demandent la justification des calculs faits par cet algorithme. Néanmoins, la loi n'a pas été plus loin et n'a pas cherché à définir de façon générale ce que serait un algorithme « loyal » ou « neutre »... ce qui est d'ailleurs très difficile à concevoir ! À l'occasion des élections présidentielles américaines récentes, de nouvelles préoccupations sont également apparues. Les algorithmes qui filtrent les flots d'actualités pour choisir celles qui seront présentées à une personne particulière (sur son réseau social, sur un moteur de recherche, etc.) se fondent sur les préférences passées de cette personne, telles qu'elle les a révélées par ses clics, ses choix... Il en résulte une « bulle de filtrage » : vous n'êtes plus exposé *in fine* qu'aux informations émanant de personnes qui sont d'accord avec vous ; vous ne voyez même plus les arguments du camp adverse. Faudrait-il, pour empêcher cela, imposer à ces algorithmes des obligations de neutralité, voire de pluralisme, comme celles que le Conseil supérieur de l'audiovisuel impose aux chaînes de télévision ? Il y a peut-être du fonctionnement de la démocratie dans une société où l'information obtenue sur Internet et par les réseaux sociaux prend une place de plus en plus grande. La réflexion juridique ne fait que commencer à ce sujet.

15. La RFA avait dû suspendre le recensement de 1983 à la suite d'une campagne de protestations contre le transfert de données sensibles (comme la religion) vers d'autres fichiers. En l'absence d'un équivalent de la loi « Informatique et libertés », la Cour constitutionnelle de Karlsruhe prononça le 15 décembre 1983 un « jugement sur le recensement » (Volkszählungsurteil) qui fit date : tout membre d'une société de droit devait pouvoir déterminer l'usage et la divulgation des données statistiques le concernant. Ce principe d'auto-détermination en matière d'information (informationnelle Selbstbestimmung) imposait de refondre les procédures de collecte et de traitement. [Source : Institut National d'études démographiques 2013 Note d'analyse de François Héran « L'Allemagne et ses minorités ou les surprises du recensement de 2011 »]

16. On pourra consulter : Rochfeld J. et Zolynski C. (2016) La « loyauté » des « plateformes ». Quelles plateformes ? Quelle loyauté ? *Dalloz IP/IT* n°11 novembre 2016

**S&S** : Le titre I de la loi pour une République Numérique instaure une nouvelle catégorie de données publiques, les « données d'intérêt général », dont l'usage est considéré comme « commun » à tous les membres de la société. Faut-il voir là une innovation juridique porteuse d'avenir ?

**JR** : Certainement : la question des « communs » se pose de plus en plus dans le droit. Deux types de problèmes ont amené cette question au premier rang des préoccupations de certains juristes, dont je fais partie. Il y a d'abord la crise environnementale internationale : elle a fait naître l'idée que certaines ressources communes de l'humanité devaient être mises « hors marché » pour faire l'objet d'une protection spécifique, qu'elles soient ou non sous la souveraineté des États. Et puis il y a la poussée numérique, l'émergence de l'information, bien « non rival »<sup>17</sup> par excellence, qui appelle le partage des usages et la création en commun. Ce sont là deux sources de renouvellement possible pour le droit, qui appellent à sortir du paradigme de la propriété « absolue », qu'elle soit privée ou publique. Vis-à-vis de la nature, il faut limiter le « pouvoir de détruire » ; s'agissant des usages numériques il faut construire des modèles qui permettent un partage. Plusieurs « modèles de communs » ont été avancés dans la période récente : Élinor Ostrom, prix « Nobel » d'économie en 2009, a décrit la gestion de ressources communes par différentes collectivités, et dégagé des conditions pour que cette gestion soit durable ; Pierre Dardot et Christian Laval, philosophes, mettent plutôt l'accent sur « l'agir commun » pour fonder la notion ; on peut citer aussi le projet (non abouti) de réforme du code civil italien en 2007, qui distinguait les « biens communs » comme ceux qui servent les droits fondamentaux des personnes, biens sur lesquels la communauté serait titulaire de droits même s'ils sont par ailleurs appropriés.

Pour en revenir aux données, la mention des données d'intérêt général dans la loi République Numérique va dans le sens de ce mouvement, de même que la disposition selon laquelle l'auteur d'une recherche scientifique financée à plus de moitié sur fonds publics peut mettre ses résultats en accès libre au terme d'une période d'embargo (6 ou 12 mois), nonobstant les conventions passées avec des éditeurs. On est là dans du « savoir commun » ! En revanche, selon moi, cette problématique ne peut pas s'appliquer aux données personnelles, pour fonder un usage collectif : on ne peut pas forcer quelqu'un à mettre en commun son intimité.

**S&S** : Pour des juristes, le domaine du numérique est en pleine évolution : ce doit être passionnant ?

**JR** : C'est passionnant, et en prise avec l'actualité : par exemple, l'arrivée explosive des « objets connectés » de la vie quotidienne va étendre encore le champ de nos préoccupations. Ce secteur des études juridiques où « ça bouge tout le temps » attire des étudiants dynamiques et curieux, qui nous aident beaucoup !

---

17. « un bien non rival » peut être utilisé par certains sans que cela diminue sa disponibilité pour les autres.