Quel droit pour les données dans une économie datacentrique ?

Par Bertrand WARUSFEL
Professeur à l'Université Paris 8, avocat au barreau de Paris (cabinet FWPA)

Dans une économie dont les innovations et la productivité reposent largement sur la production, l'échange et le traitement d'informations numérisées, les données acquièrent une valeur économique, sociale et politique croissante. Mais le corollaire de cette affirmation est que, comme toute valeur, la « data » fait l'objet d'une concurrence extrême et provoque à la fois des litiges et une demande de régulation européenne, voire internationale.
On voit donc émerger progressivement un droit des données dont nous voulons ici rendre compte synthétiquement. Ce cadre juridique reste assez hétérogène et très partiel. Mais les effets très importants (et sans doute assez perturbants) de l'exploitation et du traitement algorithmique des données dans les années à venir devraient servir d'accélérateur à la structuration de ce droit, à condition que des choix politiques clairs viennent préciser les valeurs essentielles qu'une économie numérisée doit respecter.

Différents motifs de protection des données

On ramène parfois le droit des données à la seule protection légale des données à caractère personnel, laquelle a été instaurée en France par la loi Informatique et libertés du 6 janvier 1978 et établie aujourd'hui dans toute l'Union européenne par le non moins célèbre RGPD (Règlement général de protection des données) de 2016[1]. Mais d'autres aspects ne doivent pas être négligés et peuvent reposer sur des fondements différents.

La protection des données personnelles

Le droit des données personnelles a été la première construction juridique autonome entièrement dédiée à régir les activités de traitement de l'information. Alors que dans d'autres domaines (comme les contrats, la propriété intellectuelle ou le commerce en ligne), le droit de l'informatique a préféré se construire à partir des dispositions de droit commun et de leur adaptation aux particularités du numérique, on a inventé là, de toutes pièces, un dispositif protégeant la vie privée des citoyens face aux moyens de collecte et de traitement de plus en plus puissants que la technologie numérique offre.

Pour ce faire, chaque citoyen s'est vu reconnaître un droit propre sur le traitement numérique de ses informations personnelles. Ce droit se traduit par autant d'obligations que les « responsables de traitement » (c'est-à-dire, les entités qui collectent et traitent ces données) doivent respecter, à commencer par en assurer la confidentialité et ne pas en faire une exploitation pour d'autres finalités que celle ayant justifié leur recueil ; le tout sous le contrôle d'organismes indépendants de contrôle dans chaque État européen (comme la CNIL, en France).

La protection des données professionnelles

Il existe d'autres types de données dont le traitement est juridiquement encadré. Pour s'en tenir au droit de l'Union européenne, on peut relever la directive de 1996[2] qui est venue préciser les prérogatives que peuvent revendiquer ceux qui investissent dans la constitution d'une base de données, de manière à ce que toute personne qui accède à une telle base (par exemple, à travers un service en ligne) ne puisse pas la reproduire à l'identique ou en extraire des parties substantielles. L'objectif avoué a été de préserver ainsi les entreprises européennes contre les possibilités de « parasitisme » de leur patrimoine immatériel.

Pour protéger également les entreprises européennes contre d'autres formes de détournement de leurs actifs immatériels, l'Union européenne a aussi établi en 2016 une protection juridique spéciale couvrant les différentes formes du « secret des affaires »[3]. Toute information d'une entreprise, de quelle que nature qu'elle soit (technique, commerciale, financière, stratégique…) et qui a été conservée confidentielle, peut en bénéficier pour autant que l'entreprise puisse prouver que cette information garde une valeur commerciale du fait de son caractère secret et qu'elle a fait l'objet

(1) Règlement général de protection des données 2016/279 du 27 avril 2016.

(2) Directive 96/9/CE du 11 mars 1996.

(3) Directive 2016/943 du 8 juin 2016.

« de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret »[4]. Du fait de la dématérialisation en cours du fonctionnement des entreprises, la plus grande partie des secrets d'affaires sont accessibles sous la forme de données numériques, notamment tout ce qui va toucher aux algorithmes ou aux données d'apprentissage mises en œuvre par l'entreprise pour fournir son service à ses clients.

D'autres motifs particuliers de protection des données

Pour être complet, il faut rappeler que d'autres données peuvent également couvrir des informations protégées dans des domaines sectoriels particulièrement sensibles. C'est ainsi le cas des données portant sur des informations classifiées en matière de Défense (qui touchent à la sécurité nationale des États), des données de santé ou encore de toutes les données produites ou échangées avec leurs clients par des professionnels astreints au respect du secret professionnel (médecins et avocats, pour n'évoquer qu'eux). Enfin, lorsqu'un ensemble de données numériques exprime une innovation technique ou une création originale, lesdites données deviennent alors le support de droits de propriété intellectuelle, dont le titulaire peut faire un usage exclusif et dont il peut même, sous certaines limites, restreindre l'accès.

Mais à cette forte tendance à la protection des données sous toutes leurs formes et pour différents motifs, s'oppose une orientation assez orthogonale qui pousse, au contraire, à l'ouverture et au partage des données. Cette tension juridique et politique entre protection et ouverture n'est pas en soi nouvelle, elle anime notamment tout le droit de la propriété intellectuelle (lequel protège les droits des titulaires tout en organisant les conditions de la circulation des œuvres). Mais en matière de données numériques, elle n'est qu'un aspect d'un ensemble de contradictions qu'il faudra bien un jour trancher et arbitrer.

Des logiques contradictoires entre maîtrise et ouverture des données

Consciente de l'importance croissante de toutes ces données et de la tension que leur appropriation pourrait susciter, l'Union européenne a déjà ouvert le chantier de ce qu'elle a d'abord dénommée pudiquement « les données à caractère non personnel » et de leur partage au sein de l'espace européen. Elle veut aujourd'hui aller plus loin et établir une véritable liberté de circulation de toutes les données dans l'Union, poursuivant l'ouverture déjà effective sur un autre terrain, celui des données publiques ; au risque toutefois d'accroître indirectement les injonctions contradictoires auxquelles la politique des données en Europe doit faire face.

De l'ouverture des données publiques à la libre circulation de toutes les données numériques

C'est dans un objectif de stimulation de la croissance et de défiance à l'encontre des administrations publiques (soupçonnées d'abuser de leur pouvoir informationnel pour fausser la concurrence) que l'Union européenne a adopté en 2003 une directive sur « la réutilisation des informations du secteur public »[5]. Les gisements d'informations aux mains des administrations doivent être mis à disposition des entreprises privées pour leur permettre de développer de nouveaux produits ou services. Les « jeux de données » concernés doivent être mis en ligne sous une forme anonymisée sur des serveurs (comme le site data.gouv.fr français) afin que chacun puisse en extraire la valeur intrinsèque, y compris en y appliquant des traitements algorithmiques et en les croisant avec d'autres données.

Évidemment, cette politique de l'*open data* se retrouve souvent en conflit avec différentes autres limites juridiques, que ce soit la préservation de la vie privée des citoyens, la protection des secrets protégés par la loi (comme évoqué *supra*) ou certains aspects du droit de la propriété intellectuelle[6]. Un nouveau texte dénommé Data Gouvernance Act devrait d'ailleurs être prochainement adopté au niveau européen pour mieux organiser la compatibilité entre l'ouverture des données et le respect des secrets protégés ou des droits intellectuels des tiers.

Poursuivant plus largement un objectif d'ouverture de toutes les formes de données non personnelles, une directive peu connue de 2018 a défini quelques grandes lignes du cadre juridique applicable au « libre flux » des « données à caractère non personnel » au sein de l'Union européenne[7]. Mais le véritable véhicule législatif en la matière n'est encore qu'un projet, celui du "Data Act" qui vient de faire l'objet d'un accord politique à Bruxelles et dont le principe serait d'établir une nouvelle liberté de circulation en Europe, celle des données après celle des biens, des capitaux, des services et des personnes. Sont visés, en particulier, les flux de données techniques que vont produire les équipements connectés et l'IoT. Mais là aussi l'exercice ne sera pas sans complexité, tout d'abord en ce qui concerne la distinction entre données personnelles et données non personnelles.

[4] Article 2(1) de la directive du 8 juin 2916 précitée, repris en France dans l'article L.151-1 du Code de commerce.

[5] Directive 2003/98 du 17 novembre 2003 concernant la réutilisation des informations du secteur public (aujourd'hui modifiée par la directive 2013/37 du 26 juin 2013).

[6] Voir, notamment, WARUSFEL B. (2020), « Numérisation de l'action publique et *open data* : une révolution face à ses limites », *Propriétés intellectuelles*, n°75, avril ; et WARUSFEL B. (2018), « Enjeux et limites de l'ouverture des données en matière de sécurité et de Défense », *Revue française d'administration publique*, 2018/3, n°167, pp. 551-564.

[7] Directive 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne.

D'autres contradictions à dépasser

Au carrefour des différentes normes juridiques qui s'appliquent de manière hétérogène, la donnée numérique est l'objet de logiques difficiles à concilier, voire contradictoires. Nous illustrerons ici quelques-unes des plus caractéristiques.

La première concerne la collecte des données personnelles. Comme nous l'avons déjà relevé plus haut, les réglementations françaises et européennes en matière de protection des données ont été établies pour que la personne concernée puisse échanger son consentement à la communication de ses données personnelles contre l'engagement du responsable du traitement d'en respecter la finalité et la confidentialité, et ainsi sa vie privée. Mais depuis la généralisation de l'usage d'Internet et le développement massif des communications numériques mobiles, ce n'est plus du tout ainsi que s'effectue la collecte : de ponctuelle et volontaire, elle est devenue permanente et occulte. Nul ne sait en effet la nature et le volume des données qui sont récupérées lors de chaque transaction avec un service en ligne, ni même le plus souvent qui sont le ou les prestataires de services qui en assurent la captation, le stockage, puis l'exploitation. Dès lors, derrière le paravent largement symbolique de l'autorisation préalable des *cookies* lors de la connexion à un site Web, se cache une réalité beaucoup plus cynique : celui qui souhaite bénéficier des avantages technologiques liés aux services en ligne (ou qui y est contraint) perd tout à la fois son droit à l'information et au respect de la finalité initiale de la collecte ainsi que son droit à s'opposer à (ou du moins à limiter) l'exploitation de ses propres données.

La deuxième difficulté, qui est plutôt d'ordre géo-économique, tient au fait que les États-Unis, qui sont le principal centre du cyberespace contemporain, ont jusqu'ici toujours refusé d'adopter un mécanisme de protection en ligne de la vie privée équivalent au droit européen des données personnelles. Et, là encore, le décalage entre la théorie et la pratique est flagrant : malgré la réitération par la Cour de justice de Luxembourg de sa condamnation des conditions de transfert des données personnelles vers les États-Unis[8], la collecte massive d'informations réalisée par les grandes plateformes sur les internautes européens n'a pas cessé et entraîne toujours un flux constant de données européennes à destination des États-Unis en dépit de leur refus de se doter d'un dispositif de protection équivalent au RGPD.

Conséquence indirecte de ce désaccord transatlantique profond (qui concerne aussi d'autres aspects du droit européen, comme celui des bases de données), une certaine partie de la doctrine anglosaxonne cherche à promouvoir un modèle d'appropriation privative des données personnelles (lesquelles deviendraient la propriété de chaque usager). Ce n'est pourtant pas une approche adaptée à un objet numérique qui doit à la fois demeurer en permanence sous la maîtrise de son producteur originel (puisqu'il s'agit de données qui lui sont personnellement attachées) et pouvoir être malgré tout partagé et transmis à de multiples interlocuteurs. Le véritable droit de propriété ne peut porter, au contraire, que sur une valeur dont le titulaire initial peut se défaire complètement et dont la possession peut être exclusive. La reconnaissance d'une telle propriété sur les données personnelles n'aurait pour effet que de marchandiser totalement ces données et de saper les bases théoriques du modèle européen, lequel repose sur la reconnaissance d'un simple droit de la personnalité qui ne comporte en lui-même aucune dimension patrimoniale directe.

Plus paradoxal, on peut évoquer le dilemme autour de l'usage des différentes techniques cryptographiques. Schématiquement, deux types de fonctions peuvent être mis en œuvre à partir de ces technologies de sécurité : l'une vise à l'authentification et à l'intégrité des données (notamment par des mécanismes de type signature électronique ou *blockchain*), tandis que l'autre permet d'en assurer la confidentialité par le chiffrement. Sur le principe, ces deux approches paraissent complémentaires, mais, en réalité, on s'aperçoit que deux logiques antagonistes s'opposent en arrière-plan : celle de la protection privative des données par les entreprises et les citoyens et celle des politiques sécuritaires publiques.

D'un côté, l'authentification numérique renforce certes la confiance dans les transactions électroniques et la prévention des cyberattaques, mais elle aboutit aussi logiquement à accroître la traçabilité des échanges et des personnes, ce qui peut être problématique pour le respect de la vie privée de celles-ci. De l'autre, et inversement, le recours au chiffrement par les fournisseurs de services numériques et les usagers protège efficacement leurs secrets, qu'ils soient privés ou professionnels, mais peut aussi réduire les capacités légales d'interception ou d'investigation des services des États (qu'il s'agisse de la police judiciaire ou des services de renseignement).

Une nouvelle manifestation de ces contradictions entre protection des données privées et prérogatives de la puissance publique a éclaté au grand jour avec deux arrêts de la Cour de justice de l'Union européenne d'octobre 2020[9] et d'avril 2022[10]. Faisant prévaloir le droit des données personnelles et la garantie des droits fondamentaux, les juges européens ont réduit la possibilité pour les services de renseignement d'accéder rétroactivement aux données de connexion conservées par les opérateurs de communication électronique au seul cas où la « sécurité nationale » est en jeu (ce qui couvre notamment la lutte contre le terrorisme ou l'espionnage). En revanche, la Cour a purement et simplement interdit d'utiliser ces mêmes données pour la seule lutte contre le crime organisé, estimant qu'il s'agissait d'une menace de moindre niveau qui ne justifiait pas une telle atteinte aux données personnelles des citoyens.

[8] Arrêts CJUE, 6 octobre 2015, aff. n°C-362/14 (dit « Schrems 1 ») et CJUE, 16 juillet 2020, aff. n°C311/18 (« Schrems 2 »).

[9] CJUE, arrêt La Quadrature du Net, 6 octobre 2020, aff. n°C-511/18 et autres.

[10] CJUE, arrêt Dwyer, 5 avril 2022, aff. n°C-140/20.

Conclusion : une cohérence à construire

L'adoption à venir du futur *Data Act* européen pourrait permettre de franchir symboliquement un pas significatif en donnant pour la première fois une définition – somme toute large et assez neutre – de la donnée (et non plus de certaines sous-catégories de celle-ci), qui recouvrirait « toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, y compris sous forme d'enregistrement sonore, visuel ou audiovisuel »[(11)].

Mais une simple définition ne suffit pas, encore faudra-t-il choisir et hiérarchiser les valeurs de principe qui devraient constituer les fondements du droit des données. Schématiquement, on peut en identifier quatre qui s'avèrent essentielles : le droit de contrôler l'usage de ses données ; puis celui de pouvoir en retirer de la valeur et d'en négocier contractuellement l'accès ou l'exploitation ; ensuite, le droit de les protéger techniquement et juridiquement contre ce qui peut affecter leur intégrité ou leur confidentialité ; et, enfin, la nécessité de faire prévaloir les droits de la personne sur tout traitement qui porterait atteinte à l'individu et à ses libertés fondamentales.

En effectuant de tels choix et en les articulant dans un cadre juridique cohérent, la décision politique pourrait permettre au modèle européen de régulation d'une économie datacentrique de devenir une base de négociation et d'harmonisation au plan international.

[(11)] Article 2(1) du projet de règlement « on harmonised rules on fair access to and use of data » (Data Act), 23 février 2002.