Le marché unique numérique et la régulation des données personnelles

Par Catherine BARREAU
Professeur de droit de l'entreprise à la Faculté de droit et de science politique de l'Université Rennes I

En 2015, la Commission européenne a publié une liste de 16 propositions en vue de parvenir à l'instauration d'un marché unique numérique. Selon de nombreux observateurs, le véritable trésor de ce marché réside dans les données personnelles, dont les entreprises du secteur digital font commerce. Ces données, qui relèvent de l'intimité des personnes, font l'objet d'une protection spécifique qui leur confère un statut particulier au sein tant de l'Union européenne que de chacun des États membres : elles sont l'objet d'un droit fondamental. Longtemps régie par une simple directive, cette matière sera bientôt soumise à un règlement qui a été adopté au printemps 2016. Cette nouvelle réglementation est-elle de nature à créer l'équilibre recherché entre la protection des libertés fondamentales (notamment de la vie privée des consommateurs numériques) et les besoins d'entreprises à la recherche de souplesse et de simplicité ? S'agissant d'un règlement, ce texte devrait s'appliquer de manière uniforme au sein du marché intérieur européen. Mais le règlement laisse une importante marge de manœuvre aux États membres, faisant craindre une renationalisation de la protection des données personnelles, qui pourrait constituer un obstacle à la réalisation du marché unique numérique.

La communication de la Commission européenne intitulée « Stratégie pour un marché unique numérique en Europe » (MUN) [1] définit le marché unique numérique comme « un espace dans lequel la libre circulation des biens, des personnes, des services et des capitaux est garantie… Un espace où les particuliers et les entreprises peuvent, quels que soient leur nationalité et leur lieu de résidence, accéder et se livrer à des activités en ligne dans un cadre garantissant une concurrence loyale et un niveau élevé de protection des consommateurs et des données à caractère personnel ».

Le marché mondial du numérique est aujourd'hui dominé par les GAFA [2] et seuls les YBAT [3] leur résistent efficacement. L'Europe doit résoudre un conflit entre, d'une part, la protection des données personnelles et, d'autre part, la promotion d'une logique de marché intérieur numérique qui postule la liberté du commerce des données.

Pour assurer l'efficacité de sa démarche, l'Europe doit influencer ses partenaires, en particulier la Suisse [4] et les États-Unis [5]. Des consultations publiques lancées au cours du second semestre 2015 ont permis de prendre en compte l'opinion des parties prenantes. La Commission a adopté plusieurs textes au cours du premier semestre 2016, les autres mesures le seront d'ici à la fin de l'année. Un certain retard dans l'adoption des mesures est constaté et plusieurs professionnels du secteur du numérique doutent de l'efficacité des dispositions retenues.

Juridiquement, cette initiative suscite un certain scepticisme : si la dissémination des règles relatives aux données personnelles au sein de la Stratégie MUN (que nous développons ci-après) s'avère fonctionnelle, l'inclusion dans le texte assurant la protection des données personnelles d'une logique de marché intérieur s'avère plus délicate (ce point sera développé en seconde partie de cet article).

La dissémination fonctionnelle des règles relatives aux données personnelles au sein de la Stratégie MUN

La Stratégie MUN repose sur 3 piliers dont chacun comporte 3 actions, qui déboucheront sur 16 mesures. Chacun des trois piliers comporte au moins une action relative aux données personnelles.

(1) COM(2015) 192 final.
(2) Google, Apple, Facebook, Amazon, toutes des sociétés américaines.
(3) Le russe Yandex et les chinois Baidu, Alibaba et Tencent (ce dernier étant connu pour sa messagerie WeChat).
(4) Celle-ci s'apprête à adapter sa législation pour l'articuler avec celle de l'Union européenne : http://dievolkswirtschaft.ch/fr/2015/10/2015-11-montereale/
(5) Aux États-Unis, le transfert de données personnelles est une question délicate. Après l'invalidation du Safe Harbor *en 2015 par la Cour européenne de justice, un accord politique s'esquisse (en avril 2016) sur le* Privacy Shield.

Premier pilier : l'amélioration de l'accès aux biens et aux services numériques dans toute l'Europe pour les consommateurs et les entreprises [6]

Ce premier pilier implique des propositions législatives concernant les marchés transfrontières, une réforme du régime du droit d'auteur, l'identification de problèmes de concurrence potentiels [7] et une harmonisation des différents régimes de TVA [8]. Deux propositions de directives ont été formulées en 2015 : l'une est relative à certains aspects des contrats de vente en ligne [9] et l'autre porte sur certains aspects des contrats de fourniture de contenu numérique [10]. Un paquet sur le commerce électronique a été présenté le 25 mai 2016 [11], dont un texte sur le géoblocage [12].

La législation proposée [13] garantira que les consommateurs qui cherchent à acheter des biens ou des services dans un autre pays de l'Union européenne, que ce soit en ligne ou en se rendant en personne dans un magasin, ne fassent pas l'objet d'une discrimination en termes de prix, de conditions de vente ou de modalités de paiement, sauf si celle-ci est objectivement justifiée par des motifs, tels que la TVA ou certaines dispositions légales d'intérêt public.

Par ailleurs, pour éviter une charge disproportionnée pour les entreprises, la proposition n'impose pas d'obligation de livrer dans toute l'Union européenne et exempte de certaines de ses dispositions les petites entreprises se situant au-dessous de certains seuls nationaux de TVA. Les autorités nationales pourront vérifier si des sites Internet pratiquent le blocage géographique des consommateurs. Les services de transport, les services financiers de détail, les services de l'audiovisuel, l'industrie musicale et les livres électroniques ne sont pas concernés [14] (mais le règlement fera l'objet d'une révision au bout de 2 ans, et la question de leur inclusion pourra alors être reposée).

La Commission a ensuite publié une communication intitulée « Un agenda européen pour l'économie collaborative » [15]. Les plateformes [16] doivent être en mesure de proposer leurs services dans des conditions de concurrence non faussée. Les États membres sont invités, sous le regard vigilant de la Commission, à réexaminer – et le cas échéant – à réviser leur législation en tenant compte de 5 orientations concernant les exigences en matière d'accès au marché, la responsabilité en cas de problème, la protection des utilisateurs par la législation consumériste de l'Union européenne, l'existence d'une relation de travail et les règles fiscales applicables.

Deuxième pilier : l'offre d'un « environnement propice » au développement des réseaux et des services innovants en soutenant les entreprises européennes, mais en renforçant également la protection des données personnelles

À la fin de l'année 2016, la réforme de la réglementation européenne en matière de télécommunications, la révision de la directive sur les « services de médias audiovisuels » [17], l'analyse du rôle des plateformes en ligne sur le marché (transparence des résultats de recherche), un partenariat avec l'industrie sur la cybersécurité dans le domaine des technologies et des solutions pour la sécurité des réseaux en ligne auront été proposés. La construction de ce pilier a déjà bien avancé [18], mais la mesure la plus importante en matière de régulation des données personnelles, à savoir la révision de la directive « Vie privée et communications électroniques » [19], est, quant à elle, à peine entamée [20]. Le nouveau texte qui résultera de cette révision devra être articulé avec la réforme de la protection des données personnelles.

Troisième et dernier pilier de la stratégie de la Commission : la maximisation du potentiel de croissance de l'économie numérique européenne

Ce troisième pilier comporte les initiatives relatives à la protection des données personnelles, à la libre circulation des données et à la constitution d'un *cloud* européen. Un premier train de mesures a été présenté par la Commission le 19 avril 2016 [21], lesquelles sont destinées à soutenir et à relier entre elles les initiatives nationales visant à favoriser le passage au numérique de l'industrie et des services connexes dans tous les secteurs, ainsi qu'à stimuler l'investissement au moyen de partenariats et de réseaux stratégiques. Dans ce cadre, la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

---

(6) Une enquête du Journal du Net fournit des chiffres intéressants permettant de comprendre les enjeux économiques de la question : http://www.journaldunet.com/ebusiness/commerce/1179389-la-fragmentation-legislative-et-logistique-entrave-l-e-commerce-europeen/

(7) https://ec.europa.eu/digital-single-market/en/news/first-brief-results-public-consultation-geo-blocking-and-other-geographically-based

(8) Une proposition de simplification de la TVA est prévue pour l'automne 2016.

(9) https://ec.europa.eu/transparency/regdoc/rep/1/2015/FR/1-2015-635-FR-F1-1.PDF

Grégoire LOISEAU, Communication Commerce Électronique*, 2016, commentaire n°23.*

(10) https://ec.europa.eu/transparency/regdoc/rep/1/2015/FR/1-2015-634-FR-F1-1.PDF

(11) http://europa.eu/rapid/press-release_IP-16-1887_fr.htm

(12) Illustrée par l'affaire Disneyland, par exemple.

(13) http://ec.europa.eu/DocsRoom/documents/16742

(14) Par exemple, en France, les chaînes de télévision financent le cinéma.

(15) http://ec.europa.eu/DocsRoom/documents/16881

(16) Au sens de la directive Commerce électronique 2001/31/CE, ce sont des fournisseurs d'hébergement.

(17) Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010.

(18) Le 17 mai 2016, le Conseil de l'Union européenne a validé le compromis sur la cybersécurité (Bull. quot. Europe, n°11552 du 18 mai 2016) : http://www.consilium.europa.eu/fr/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/; et, le 25 mai 2016, la Commission a entrepris la révision de la directive SMA : ec.europa.eu/digital-single-market/en/news/proposal-updated-audiovisual-media-services-directive

(19) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive Vie privée et communications électroniques) : JOUE, 31 juillet 2002, L201/37.

(20) ec.europa.eu/eusurvey/runner/1710fec6-2226-4116-8bc0-a29829d7e1bf?draftid=7eaa51c7-dac9-4c36-8406-7a465a729f6e&surveylanguage=FR

(consultation publique réalisée en ligne entre le 11 avril et le 5 juillet 2016).

(21) europa.eu/rapid/press-release_IP-16-1407_fr.htm

et à leur libre circulation a été révisée. Mais cette réforme angulaire tient-elle le pari d'inclure la stratégie MUN ?

Une inclusion minimaliste de la stratégie MUN dans le RGPD (Règlement général de protection des données personnelles)

Le Traité sur l'Union européenne (TUE) a conféré à la protection des données personnelles le caractère d'un nouveau droit fondamental, concrétisant ainsi l'article 8 de la Charte européenne des droits fondamentaux. L'article 16 du Traité sur le fonctionnement de l'Union européenne (TFUE) confirme ce droit et prévoit qu'il appartient au Parlement européen et au Conseil d'adopter les règles relatives à la protection des personnes à l'égard du traitement de leurs données personnelles et de leur libre circulation. Le règlement (UE) 2016/679 a été adopté le 27 avril 2016 et publié au Journal Officiel de l'Union européenne (JOUE) le 4 mai 2016 (L119/1) [22]. Entré en vigueur 20 jours après sa publication, il remplacera la directive 95/46/CE dans deux ans. Le considérant 171 du règlement confirme le fait que le passage d'une régulation à l'autre ne sera pas brutal. Les traitements en cours à la date d'application du Règlement général de protection des données personnelles (RGPD) devront être mis en conformité avec celui-ci dans un délai de deux ans après son entrée en vigueur. Malgré son ambition, le RGPD a été adopté dans une version de compromis, différant parfois fortement des versions de travail du fait d'un intense déploiement d'activité de la part de certains *lobbies* dont l'influence est nettement perceptible. Il laisse une étonnante marge de manœuvre aux États membres, résultat de compromissions qui risquent de menacer le succès de la Stratégie MUN.

De prime abord, le RGPD est un texte visant à assurer la protection des personnes, il semble donc peu favorable à la marchandisation des données personnelles. Mais une dimension « marché intérieur » est détectable dans certaines de ses dispositions

La lecture du RGPD révèle une continuité entre l'ancienne et la nouvelle régulation. Les définitions de base de la directive ont été maintenues (art. 4), les droits des personnes concernées sont approfondis et augmentés, et les obligations des responsables de traitement renouvelées.

Les traitements de données personnelles ne sont licites que si la personne concernée y a consenti clairement et explicitement, après avoir été informée précisément et dans un langage simple et clair des finalités du traitement. Elle peut s'opposer au profilage et invoquer un véritable droit à l'oubli encore plus solide que le droit au déréférencement reconnu par la CJUE dans l'arrêt « Google ».

Le droit à la portabilité des données (pour permettre notamment les changements de fournisseur) est consacré. Les conditions du transfert des données collectées dans les pays tiers sont strictes. Ces droits s'exercent gratuitement. Parallèlement, les entreprises doivent protéger les données dès la définition des moyens de leur traitement en recourant à la technique de la *privacy by design*, laquelle consiste à respecter un principe de sécurité par défaut. Les entreprises sont tenues de désigner en interne des « délégués à la protection des données », d'adopter des codes de conduite, de respecter des mécanismes de certification et de notifier obligatoirement les failles dans la sécurité à l'autorité de contrôle et aux personnes concernées. Selon la violation constatée, la sanction est une amende administrative pouvant s'élever jusqu'à 10 000 000 d'euros ou 20 000 000 d'euros ou, dans le cas d'une entreprise, de 2 à 4 % de son chiffre d'affaires annuel mondial total de l'exercice précédent (le montant le plus élevé étant retenu).

Ces règles illustrent la volonté de la Commission, qui est le reflet de celle exprimée par la société civile lors de consultations publiques, de restaurer, au profit des personnes concernées, la maîtrise des données les concernant. Mais l'efficacité des mesures prises n'est pas certaine. En ce qui concerne les exigences relatives au consentement, s'appliqueront-elles, dès lors qu'aujourd'hui le consentement demandé a pu apparaître illusoire ? [23] La technique de la *privacy by design* ne serait pas une régulation vraiment efficace [24], car la pseudonymisation ne serait pas vraiment protectrice [25]. On ajoutera que le RGDP ne répond pas aux problématiques que soulèvent les *Big Data* [26].

Les entreprises ont élevé assez peu de protestations contre ce texte, dont la publication a reçu peu d'écho (notamment dans la presse française). Certaines études indiquent que les entreprises ignorent même l'existence de cette nouvelle réglementation. Celle-ci offre pourtant un cadre plus propice à la stratégie MUN. Ainsi, les dispositions relatives au champ d'application extraterritorial confèrent à ces entreprises de nouveaux moyens de résistance face aux GAFA.

Le RGDP est applicable aux responsables de traitement de données établis dans l'Union européenne et aux responsables établis en dehors de l'Union européenne, si ce traitement vise des résidents de l'Union européenne (art. 3). C'est l'une des nouveautés les plus remarquables qui renforcera l'autorité de l'Union européenne pour négocier avec les entreprises et les autorités publiques extra-européennes.

Cette disposition risque d'être ressentie par des États tiers comme une atteinte à leur souveraineté. Sachant toutefois que les pouvoirs de contrôle et de coercition des autorités de l'Union européenne et des États membres ne peuvent être exercés en dehors du territoire de l'Union européenne.

---

(22) Le paquet sur la protection des données inclut également une directive relative aux transferts de données à des fins policières et judiciaires.

(23) BOIZARD (M.), « Le consentement à l'exploitation des données à caractère personnel : une douce illusion ? », Communication Commerce Électronique*, n°3, étude 6, mars 2016.*

(24) RALLET (A.), « De la privacy by Design à la Privacy by using », Regards croisés Droit/économie*, Réseaux 2015/1, n°89, pp. 15-46.*

(25) wiki.laquadrature.net/Synth%C3%A8se_du_r%C3%A8glement_sur_la_protection_des_donn%C3%A9es/en

(26) VULLIET-TAVERNIER (S.), « Big Data et protection des données personnelles : quels enjeux ? (éléments de réflexion) », Statistique et société*, vol. 2, n°4, décembre 2014, p. 27 sq ; MAYER-SCHÖNBERGER (V.), « La Révolution Big Data »,* Politique étrangère*, 2014/4, pp. 69-81.*

Si la situation est donc clarifiée par rapport à celle qui résultait de la jurisprudence Google, les entreprises européennes ne peuvent pas pour autant espérer être placées sur un pied de parfaite égalité avec les entreprises américaines.

En effet, si les responsables et sous-traitants établis hors de l'Union européenne doivent désigner par écrit un représentant (art. 27), cette obligation ne s'applique ni en cas de traitement occasionnel ni aux autorités publiques. Au lieu de contribuer à l'efficacité de la réglementation européenne, cette disposition, en raison des contours flous de la première exception, peut devenir une source d'insécurité juridique, en conférant aux entreprises étrangères le soin de déterminer par elles-mêmes si elles sont soumises ou non aux obligations du RGDP. La dimension politique de la seconde exception en explique le caractère très général. D'importantes difficultés diplomatiques auraient en effet pu résulter de la solution inverse. Seule la mise en place d'un cadre international conventionnel de protection des données personnelles permettra (dans un futur lointain et incertain) d'assurer la protection des personnes concernées.

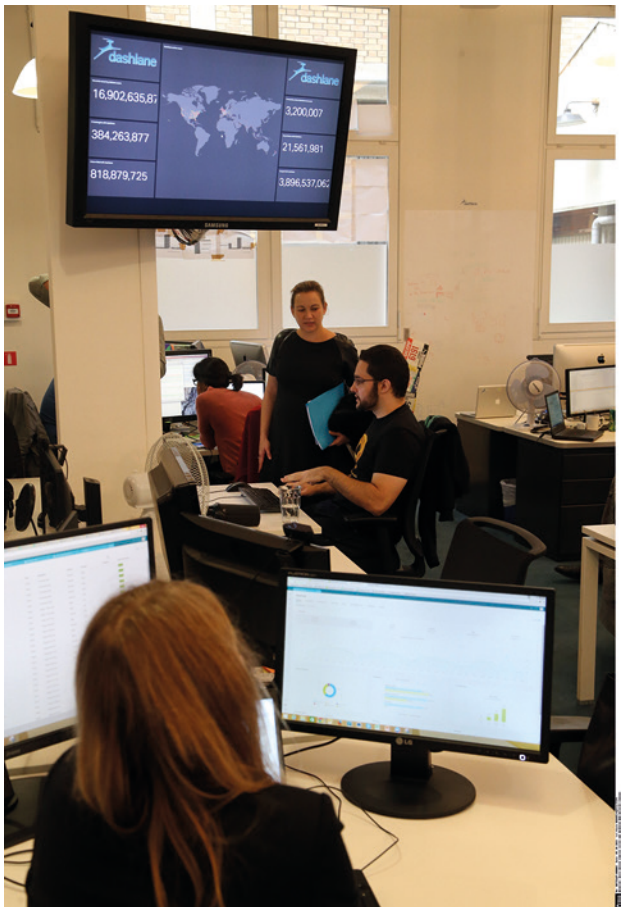

Photo © Alain Robert/APERÇU-SIPA

Axelle Lemaire, secrétaire d'État chargée du Numérique, visitant la société Dashlane qui propose des solutions innovantes de protection des données, Paris, octobre 2015.

« Les institutions de l'Union européenne, les États membres et leurs autorités de contrôle sont toutefois encouragés à "prendre en considération les besoins spécifiques des PME" ».

Par ailleurs, les entreprises disposeront d'un mécanisme de guichet unique. Elles auront une seule autorité de contrôle comme interlocuteur chef de file chargé d'appliquer les règles du RGDP. Cette simplification est la bienvenue pour les PME qui ne bénéficient pas d'une exemption générale des dispositions du RGDP. L'article 31-5 tient seulement compte de leur situation en organisant, en ce qui concerne la tenue de registres, une dérogation pour les organisations occupant moins de 250 employés. Les institutions de l'Union européenne, les États membres et leurs autorités de contrôle sont toutefois encouragés à « prendre en considération les besoins spécifiques des PME ». Il s'agit là d'une invitation faite aux États à utiliser la marge de manœuvre que leur laisse le RGDP.

Bien qu'un règlement, en tant que loi européenne, soit, dans toutes ses dispositions, applicable à tous dans tous les États membres, le RGDP laisse à ces derniers la possibilité d'adopter leurs propres dispositions. Il est d'ailleurs à noter que certains éléments essentiels sont affichés dans les considérants et non dans le texte même du RGDP

Parce qu'une régulation uniforme des données personnelles assure un niveau cohérent de protection des personnes physiques dans l'ensemble de l'Union et évite que des divergences nationales n'entravent le libre flux de ces données au sein du marché intérieur, le règlement a été préféré à la directive.

Le Considérant 9 rappelle ces principes. Mais ceux-ci sont aussitôt relativisés par le Considérant 10, qui confère aux États membres la possibilité de déroger au RGDP en réglementant un grand nombre de traitements sur une base spécifique et nationale.

Cette marge de manœuvre leur est reconnue en ce qui concerne le traitement de données à caractère personnel nécessaire au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ou le traitement de catégories particulières de données à caractère personnel (notamment des données dites « sensibles »).

Une brèche importante dans le processus d'unification des règles au niveau européen est ainsi ouverte non seulement au regard de règles très spéciales, mais aussi sur des points communs, dont il aurait semblé (au vu des objectifs annoncés) qu'ils auraient dû relever par essence du champ de l'uniformisation.

Le risque est réel que les États adoptent des mesures qui éloignent les uns des autres les droits nationaux tout autant qu'ils le sont aujourd'hui, voire davantage, engendrant une insécurité juridique pour les entreprises [27], qui devront tenir compte des spécificités de chaque État membre afin de s'assurer de la légalité de leurs traitements de données personnelles – contrairement au principe même du « guichet unique » que le RGDP promet par ailleurs.

(27) www.businesseurope.eu/sites/buseur/files/media/press_releases/2016-04-14_pess_release_on_data_protection_regulation.pdf

Ce risque d'une divergence entre les législations des États membres peut être limité par l'exigence de l'article 36-4, aux termes duquel les États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une règle relative au traitement de données personnelles.

Les autorités de contrôle travaillent en effet en étroite concertation et pourront donc attirer l'attention des États sur des écarts législatifs potentiels et sur leurs conséquences éventuelles. Ces autorités de contrôle coopéreront, s'assisteront mutuellement, voire seront amenées à agir conjointement (art. 60 et s.). Il existe également un mécanisme de contrôle de la cohérence (art. 63), dont le fonctionnement est placé sous l'égide d'un Comité européen de protection des données, dont la composition et les attributions sont définies aux articles 68 et s.

Le RGDP comporte par ailleurs une longue liste de considérants.

Par nature dépourvus d'effet obligatoire, ces considérants incluent parfois des mesures qui auraient pu figurer dans les articles mêmes du texte, si un accord avait pu être trouvé. En résulte-t-il aussi un risque de renationalisation rampante, au détriment du marché unique numérique ? Une attention particulière doit être apportée au Considérant 53, qui est nécessaire à la compréhension de l'article 17 sur le droit à l'oubli. Cette disposition aurait dû comprendre en elle-même tous les éléments nécessaires à sa mise en œuvre, dans l'intérêt tant des personnes concernées que dans celui des entreprises. Il faudra attendre que la Cour de justice de l'Union européenne (CJUE) se prononce sur ce point pour lever ces incertitudes.