L'EUROPE NUMÉRIQUE

L’Europe, le cyberespace et la protection des données

Gregory VOSS

RÉSUMÉ

Le développement de l’informatique a suscité des inquiétudes quant à la vie privée des individus dont les données personnelles étaient traitées. Les nations européennes n’ont pas tardé à adopter des lois de protection des données pour préserver la vie privée des personnes physiques, ce qui a abouti à une réglementation de ce que l’on appelle le « cyberespace ». Afin de concilier la libre circulation des données en son sein avec la protection de la vie privée, l’Union européenne adopte en 1995 une législation communautaire sur la protection des données qui est par la suite intégrée dans le droit des États membres.

L’apparition de nouvelles technologies et les disparités législatives entre les États membres poussent l’Union à adopter une législation uniforme s’appliquant au niveau international, le Règlement général de protection des données (RGPD). Celui-ci renforce les droits des individus. Aux restrictions préexistantes sur les transferts de données à l’étranger s’est ajoutée une dimension clairement extraterritoriale de la loi quand les données personnelles de citoyens de l’UE sont collectées, ce qui prend acte du fait que le cyberespace ne connaît pas de frontières.

Le RGPD : une adaptation nécessaire au cyberespace

L'essor de l'informatique au cours des années 1960 et 1970 suscite l'inquiétude chez certains responsables politiques ainsi que parmi les informaticiens et les juristes, en raison des risques qu'il présente pour la vie privée des individus dont les données personnelles sont traitées. Ces données, stockées sur un ordinateur pour un coût relativement modique, peuvent être aisément récupérées. L'augmentation de la capacité de stockage sur des supports dont la taille ne cesse de se réduire, conjuguée au fait que l'on peut faire des recherches croisées sur des individus à partir de plusieurs sources, soulève la question de la protection de la vie privée, que l'information soit détenue par des gouvernements ou par des organismes privés.

Les pouvoirs publics prennent rapidement conscience de la nécessité de réglementer le traitement informatique des données sur les personnes physiques. Dès les années 1970, certains pays européens adoptent des lois sur la protection des données, en vertu du droit à la vie privée garanti par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (1959). Le land allemand de Hesse est le premier à se doter de ce type de législation, bientôt suivi par la Suède en 1973 et la République fédérale d'Allemagne en 1977, puis par la France, l'Autriche, le Danemark et la Norvège en 1978. Ces textes peuvent être présentés comme la première génération de lois sur la protection des données.

À l'origine, Internet était perçu comme un espace de relative liberté – non seulement parce que ses utilisateurs pouvaient communiquer plus ou moins anonymement, mais aussi parce que cet espace échappait à toute réglementation étatique. On parla de « cyberespace » pour qualifier ce nouveau monde de réseaux d'ordinateurs en ligne auquel sont venus s'ajouter de nouveaux appareils comme les smartphones et les tablettes. Couvrant l'ensemble de la planète, le cyberespace ignore les frontières nationales. Toutefois, comme nous l'avons vu, les États entreprennent de le réglementer, comme c'est déjà le cas pour le monde physique.

En 1995, une proposition de directive sur la protection des données personnelles, destinée à lever les obstacles à leur libre circulation au sein de l'Union européenne, est adoptée par le Parlement européen et le Conseil (directive 95/46). Elle est ensuite intégrée dans le droit des États membres pour constituer ce qu'on appelle la deuxième génération de lois sur la protection des données. Si la suppression des barrières à l'intérieur du Marché commun est la principale compétence législative de l'Union européenne, le droit au respect de la vie

privée est pris en compte au même titre que la libre circulation des données personnelles. Toutefois, le développement ultérieur de nouvelles technologies n'a pas été anticipé dans la directive, dont la transposition dans le droit des États membres présente des disparités. Cela conduit la Commission européenne à proposer l'adoption d'une nouvelle loi en 2012, le Règlement général de protection des données (RGPD). Une Charte des droits fondamentaux de l'Union européenne a déjà été adoptée en 2000. Amendée en 2007, cette charte, qui devient juridiquement contraignante avec l'entrée en vigueur du traité de Nice en 2009, inclut un droit spécifique à la protection des données. S'ajoute à cela la directive 2002/58 sur la protection des données dans le secteur des communications électroniques. Amendée en 2009, elle fait de nouveau l'objet d'une procédure de révision au Parlement sur proposition de la Commission.

Le contexte de l'adoption du RGPD

Le RGPD est proposé à une époque où la baisse des prix permet à un large public d'acquérir des ordinateurs personnels connectés au cyberespace, le nombre de personnes ayant une connexion internet passant de 64 % en 2009 à 90 % en 2019 de la population de l'Union européenne. Cela peut changer la nature des transactions commerciales et les entreprises comprennent l'intérêt qu'elles peuvent tirer du cyberespace grâce au e-commerce, c'est-à-dire la commande en ligne de biens ou de services. On estime que 64,7 % de la population de l'Union y a recours en 2020, contre 20,4 % en 2004. Après avoir connu un démarrage très lent par rapport aux États-Unis, les achats en ligne connaissent une progression spectaculaire en Europe, passant d'un milliard de dollars en 1998 à 465 milliards en 2021, selon les prévisions.

Grâce à des fichiers appelés « cookies », certaines entreprises peuvent mémoriser les achats et l'historique de navigation des visiteurs de leur site. Les cookies, apparus en 1995, mais dont l'existence n'est connue du public qu'en 1996, permettent de mieux gérer les relations avec la clientèle et de cibler les recommandations d'achats en fonction du profil de l'utilisateur. Leur utilisation est encadrée par la directive 2002/58. Mais une autre forme de commercialisation se développe avec l'offre de services gratuits, et les internautes prennent l'habitude d'avoir accès à des contenus et des prestations sans rien débourser. Le moteur de recherche gratuit de Google, fondé en 1998, en est l'exemple le plus emblématique.

Toutefois, ce type de transaction n'est pas totalement désintéressé, car les fournisseurs de services peuvent vendre la liste de leurs utilisateurs à des annonceurs publicitaires. Les entreprises prennent l'habitude de collecter des données personnelles afin d'établir des profils d'utilisateurs et d'avoir une offre publicitaire ciblée. Cela permet à des entreprises technologiques, notamment le moteur de recherche Google et le réseau social Facebook, de dominer le marché de la publicité en ligne.

La législation sur la protection des données est peu contraignante pour les géants américains de la Tech tant que ceux-ci opèrent sur le territoire des États-Unis et qu'ils ne contreviennent pas à leurs propres engagements en matière de confidentialité. Le RGPD est donc conçu comme un outil de rééquilibrage entre les entreprises européennes et leurs concurrentes soumises à des régimes juridiques plus laxistes, notamment celui des États-Unis. Il stipule en effet que toute entreprise technologique fournissant des biens ou des services aux consommateurs européens serait soumise aux mêmes règles de protection des données qu'une entreprise ayant son siège dans l'Union européenne. La mise en œuvre du RGPD

repose donc sur le principe d'extraterritorialité, puisqu'il s'applique à des entreprises dont le siège est situé en dehors des frontières de l'UE dès que celles-ci collectent les données personnelles de ressortissants de l'Union, même si ces données sont traitées en dehors de son territoire. Est donc pris en compte le fait que le cyberespace ne connaît pas de frontières.

Les révélations d'Edward Snowden sur les programmes de surveillance de l'Agence américaine de sécurité nationale (NSA) ont une incidence sur le processus législatif, car plusieurs géants américains de la Tech collaborent, à des degrés divers, avec la NSA. L'émoi suscité par cette affaire empêche les lobbies de peser sur les travaux de la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE), chargée d'élaborer la proposition législative. Un accord est rapidement trouvé sur le texte à présenter. Dès mars 2014, le RGPD est adopté en première lecture par le Parlement européen. Mais il faut attendre juin 2015 pour que le Conseil parvienne à une position commune, et les négociations tripartites entre la Commission, le Parlement et le Conseil ne débouchent sur un accord politique qu'en décembre 2015. Le RGPD est adopté en avril 2016, promulgué le mois suivant et entre en vigueur deux ans plus tard, le 25 mai 2018. Il constitue le socle de ce qu'on peut appeler, avec sa transposition dans le droit des États membres, la troisième génération de lois sur la protection des données.

Le périmètre du RGPD et son application dans le cyberespace

Le RGPD fait suite à la directive européenne 95/46 sur la protection des données ; mais à la différence d'une directive, acte législatif qui fixe des objectifs tout en laissant chaque pays libre d'élaborer ses propres méthodes pour les atteindre, un règlement est une législation contraignante qui s'applique dans tous les États. Il en existe un autre relatif à la protection des données, le règlement 45/2001, qui porte sur le traitement des données par les institutions européennes. Il est remplacé par le règlement (UE) 2018/1725 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union européenne.

Le principe de la protection des données à caractère personnel est déjà présent dans la directive européenne 95/46, mais le RGPD va plus loin. Des garanties supplémentaires sont exigées sur la nature des données et leur sécurité. Les personnes physiques concernées doivent être clairement informées de la collecte et du traitement de leurs données personnelles ; leurs droits doivent être respectés. Est passible de poursuites tout manquement aux exigences de protection des données ainsi qu'à la légalité et l'équité de leur traitement. Aux droits existants, comme l'accès à ses propres données personnelles, à leur rectification, à leur effacement quand l'objectif de leur saisie et de leur traitement est atteint, s'ajoutent le « droit à l'oubli » et le droit à la portabilité des données.

La directive 95/46 stipule simplement que le traitement des données doit être déclaré au préalable, mais le RGPD met également l'accent sur la responsabilité des contrôleurs (qui déterminent les finalités, les conditions et les moyens du traitement des données) et des processeurs (qui traitent les données pour les contrôleurs et selon leurs instructions). Ceux-ci doivent être en mesure de prouver à tout moment qu'ils sont en conformité avec les exigences de la RGPD. Les autres obligations liées à la nouvelle réglementation comprennent l'obligation de tenir un registre des activités de traitement de données, avec une exemption pour les PME, et d'avoir un délégué à la protection des données chargé de veiller à la conformité au RGPD. En outre, contrairement à la directive 95/46, le RGPD s'applique entre

autres à la biotechnologie, à la géolocalisation ainsi qu'aux données génétiques. Le RGPD instaure par ailleurs une exigence de notification de violations des données personnelles. Ces violations peuvent entraîner de lourdes sanctions administratives, dont l'effet est bien plus dissuasif que ce que prévoit la directive.

Pour qu'une procédure de traitement des données puisse relever du RGPD, elle doit répondre à certains critères. Les données doivent se rapporter à une personne vivante, désignée comme la « personne concernée ». Toutefois, le RGPD ne s'applique pas en cas d'exception domestique, c'est-à-dire quand les données traitées ont des finalités exclusivement personnelles ou domestiques, sans rapport avec une activité professionnelle ou commerciale. Il ne s'applique pas non plus aux données de personnes décédées ou de personnes morales. N'entre pas non plus dans le champ du RGPD le traitement des données à caractère personnel par les autorités compétentes 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, qui est couvert par la directive (EU) 2016/680, adoptée dans le même paquet législatif que le RGPD.

Au-delà de ces critères, reste à définir le champ d'application territorial du RGPD. Celui-ci s'applique quand les données traitées concernent les activités d'un établissement de l'Union européenne, quel que soit le lieu où le traitement est effectué. En outre, si un contrôleur (ou des processeurs) a pour objectif la vente de biens ou de services à des résidents de l'Union européenne (même en l'absence de paiement), ou s'il surveille leur comportement dans l'Union européenne, le RGPD s'applique, que le contrôleur ou le processeur soit installé dans l'Union ou non. Le contrôleur ou le processeur devra alors désigner un représentant dans l'Union européenne qui servira d'interlocuteur avec les autorités de contrôle.

Les entreprises et les institutions européennes sont couvertes par le Règlement de protection des données dans l'Union (EUPDR). Pour les autres entreprises et organismes officiels, si leur activité de traitement de données personnelles entre dans le champ d'application du RGPD, elles devront justifier d'un fondement légitime pour cela, que les personnes concernées soient des citoyens de l'Union européenne ou non. Peuvent être considérés comme fondement légitime, entre autres, le consentement d'une personne physique à l'utilisation de ses propres données personnelles, ou l'existence d'un contrat rendant nécessaire l'utilisation des données personnelles d'un des contractants.

Prenant acte du fait que le cyberespace ne s'arrête pas aux frontières de l'Union européenne, le RGPD comporte une restriction déjà présente dans la directive. Il est ainsi stipulé que des données ne peuvent être transférées à un pays tiers de l'UE ou à une organisation internationale que si le pays ou l'organisation en question a été reconnu par la Commission européenne comme offrant un niveau adéquat de protection des données à caractère personnel, faute de quoi des garanties suffisantes devront être fournies. Ces garanties comprennent des « clauses contractuelles type » homologuées par la Commission, des « règles d'entreprise contraignantes » homologuées par les autorités de contrôle compétentes, des codes de conduite et des mécanismes de certification ainsi que d'autres instruments juridiquement contraignants à la disposition des pouvoirs publics et des organismes officiels.

À deux reprises, en 2000, puis en 2016, la Commission européenne publie des décisions d'adéquation fondées sur des accords bilatéraux avec les États-Unis. Elles établissent un

cadre dans lequel les entreprises peuvent auto-certifier leur adhésion à des principes garantissant aux personnes dont les données sont transférées aux États-Unis une protection similaire à celle du droit européen. Ces deux décisions sont invalidées par la Cour de justice de l'Union européenne (CJUE) à la suite de poursuites engagées contre Facebook auprès de la justice irlandaise par un ressortissant autrichien, Maximilian Schrems, au sujet du transfert de ses données personnelles aux États-Unis. En effet, comme l'ont montré les révélations de Snowden, les pouvoirs publics américains peuvent avoir accès à ces données, à des fins de surveillance, sans respecter les garanties procédurales prévues dans le droit communautaire. La première de ces actions en justice (*Schrems I*) concerne le mécanisme d'adéquation Safe Harbor, négocié entre les États-Unis et l'Union européenne, qui est invalidé par la CJUE en octobre 2015. La seconde (*Schrems II*) vise essentiellement le recours aux clauses contractuelles type mais, en juillet 2020, la CJEU profite de l'occasion pour invalider le successeur de Safe Harbor, le Bouclier de protection des données UE-États-Unis. En 2021, les négociations se poursuivent entre les États-Unis et la Commission pour trouver un remplacement au Bouclier de protection.

Il est à noter que, si les clauses contractuelles type ne sont pas invalidées en tant que telles par Schrems II, les exigences de la CJUE sont renforcées en matière de garanties du respect de ces clauses par l'importateur de données dans le cadre de la législation et des usages de son pays. Certains commentateurs juridiques ont vu dans cet arrêt une manière d'imposer « en douceur » le stockage des données dans l'Union européenne, par opposition aux méthodes plus brutales qui prévalent dans certains pays comme la Russie ou la Chine. Il est vrai que, même si ce n'est pas obligatoire, le recours à des fournisseurs de services européens pour traiter des données personnelles venant de l'Union européenne simplifie la mise en conformité des entreprises.

Le rôle du RGPD ne se limite pas au contrôle de certaines activités des particuliers et des entreprises dans le cyberespace, y compris dans des pays tiers pour les offres de biens ou de services à destination de l'Union européenne. Il constitue en fait une sorte de *soft power* européen, grâce à l'imposition de ses normes à travers le monde. L'« effet bruxellois », pour reprendre le terme forgé par Anu Bradford, recouvre des domaines où l'Union européenne a établi des règles rigoureuses. C'est le cas de cibles inélastiques comme les marchés de consommateurs, où il est de l'intérêt des acteurs économiques comme les multinationales de s'adapter à une norme mondiale, plutôt que de tenter de tirer parti de normes moins rigoureuses ailleurs en pratiquant une politique du coup par coup. La taille et la richesse du marché européen renforcent probablement cet intérêt. On peut penser qu'une fois que des entreprises internationales adoptent les normes européennes, qui sont les plus exigeantes, elles cherchent à faire adopter des normes comparables aux autres juridictions, afin d'être « à armes égales » face à la concurrence. À la puissance du marché vient s'ajouter celle de la norme.

La nomenclature juridique unique offerte par le RGPD en matière de protection des données présente un avantage pour les entreprises comme pour les particuliers et les organismes officiels, d'autant plus que le Comité européen de la protection des données fournit des aides à l'interprétation de chaque détail de ce texte fondé sur le code civil. Le fait qu'il soit disponible en plusieurs langues, notamment en français, en anglais et en espagnol, constitue un autre avantage. C'est pourquoi de nombreux pays d'Amérique latine, d'Afrique et d'Asie choisissent de s'inspirer du RGPD et du texte qui l'a précédé, la directive 95/46, pour rédiger leur propre législation, de préférence à une démarche sectorielle comme celle des États-Unis.

La volonté institutionnelle d'exporter les normes au-delà de l'Union européenne, d'où découle ce qu'on a appelé l'harmonisation sur la base des traités, contribue également à la diffusion du modèle européen. L'inclusion de la question de la protection des données dans toute nouvelle négociation d'accord commercial, comme ce fut le cas avec le Japon en 2018 par exemple, en offre une bonne illustration. Cela peut même concerner des accords préexistants, comme ce fut le cas en juillet 2021 lorsque la Commission européenne a approuvé l'ajout d'une décision d'adéquation conforme au RGPD à l'accord de libre-échange avec la Corée du Sud. De même, la Commission a laissé entendre en 2017 que les pays d'Amérique latine (notamment les membres du Mercosur) et l'Inde pourraient être invités à négocier leurs conditions d'adéquation.

Certains juristes et commentateurs technologiques estiment toutefois que la réglementation sur les données personnelles est à l'origine du retard de l'Union européenne par rapport à d'autres blocs comme la Chine et les États-Unis en matière de nouvelles technologies, notamment le *Big Data*, l'intelligence artificielle et l'apprentissage automatique. Ils soutiennent que la réglementation constitue une entrave à l'innovation, ce qui expliquerait les difficultés de l'Europe à faire émerger ses propres géants de la Tech. Est-ce vraiment le cas ? Les autres blocs seront-ils au contraire amenés à encadrer eux aussi le développement des nouvelles technologies en reconnaissant le droit fondamental à la protection des données et en adoptant leur propre règlement général, afin de prendre en compte les questions d'éthique en matière de technologie ? L'avenir seul le dira.

BIBLIOGRAPHIE

BRADFORD, Anu, *The Brussels Effect. How the European Union Rules the World,* New York, Oxford University Press, 2020.

GONZ□LEZ FUSTER, Gloria, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham, Springer, 2014.

LYNSKEY, Orla, *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press, 2015.

VOSS, W. Gregory, « Cross-Border Data Flows, the GDPR, and Data Governance », *Washington International Law Journal*, n° 29, 2020, p. 485-531.

VOSS, W. Gregory, « European Union Data Privacy Law Reform : General Data Protection Regulation, Privacy Shield, and the Right to Delisting », *Business Lawyer,* n° 72, hiver 2016-2017, p. 221-233.

VOSS, W. Gregory, « Obstacles to Transatlantic Harmonization of Data Privacy Law in Context », *University of Illinois Journal of Law, Technology & Policy,* 2019, p. 405-463.
