Règlement général sur la protection des données et *Open Data*: enjeux et perspectives

Maximilien Lanna

In questo articolo, si tenta di determinare l'impatto che il nuovo Regolamento generale sulla protezione dei dati avrà sui dati pubblici in possesso delle pubbliche amministrazioni e se ne limiterà o favorirà la diffusione. Questa nuova serie di norme non solo obbligherà le pubbliche amministrazioni ad adottare nuove politiche quando raccolgono dati personali, ma avrà anche un impatto sul modo in cui esse diffondono i dati prima del loro stesso riutilizzo da parte di enti pubblici o privati. Piuttosto che seguire un approccio negativo, con questo articolo si cercherà pertanto di analizzare le opportunità che il nuovo quadro giuridico porterà allo sviluppo degli open data.

1. *Introduction*

Ouverture des données publiques et protection des données à caractère personnel sont deux matières qui ont longtemps eu tendance à se développer de façon séparée et sans se rencontrer. En France, les éléments de législation qui sont venus encadrer chacun de ces deux domaines sont pourtant apparus simultanément: le 6 janvier 1978 pour la loi Informatique et Libertés[1] permettant d'encadrer les traitements de données à caractère personnel et le 17 juillet 1978 pour la loi dite loi « CADA »[2] relative à l'accès aux documents administratifs. Des éléments de convergence ont pourtant progressivement vu le jour et des interactions entre les deux matières ont été inévitables[3]. Cette rencontre progressive est née

(1) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

(2) Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal

(3) G. GORCE, F. PILLET, *La protection des données personnelles dans l'open data: une exigence et une opportunité, Rapport d'information du Sénat fait au nom de la commission des lois*, n°

de l'informatisation de notre société et de l'adoption à grande échelle d'outils informatiques à la fois au sein des administrations mais également au sein des foyers. Les informations publiques, mises à disposition par l'administration sous forme de données numériques et entendues par le désormais défunt groupe de l'article 29 comme « toutes les informations du secteur public accessibles au public en vertu du droit national »[4] ont donc progressivement été appelés à contenir des informations relatives aux individus.

Le cadre juridique européen a progressivement pris en compte ce changement de paradigme. L'entrée des données à caractère personnel dans le champ des informations susceptibles d'être mises à disposition par les administrations a nécessité une adaptation du cadre juridique et c'est au niveau européen que cette impulsion a eu lieu. La directive 2003/98/CE du 17 novembre 2003[5] a permis d'intégrer les questions relatives à la protection des données à caractère personnel au domaine de la réutilisation des informations du secteur public : celle-ci devait être mise en œuvre et appliquée « dans le respect total des principes relatifs à la protection des données à caractère personnel, conformément à la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 ». Le cadre réglementaire français instauré en 1978 par la loi « CADA » a donc pris en compte ces problématiques, grâce à la transposition de la directive de 2003 par une ordonnance du 6 juin 2005. La loi pour une République numérique[6] n'a pas consacré, en tant que telle, la notion d'*open data*, mais elle en détermine le spectre et précise les modalités de mises à disposition d'informations détenues par les administrations publiques en procédant notamment à une réforme du Code des relations entre le public et l'administration[7].

469, 2014, p. 25.

(4) G29, Avis 06/2013, p. 2.

(5) Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public.

(6) Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

(7) L'article L. 300-2 du CRPA détermine ainsi quels sont les documents susceptibles d'être mis à disposition: « Sont considérés comme documents administratifs, au sens des titres Ier, III et IV du présent livre, quels que soient leur date, leur lieu de conservation, leur forme et leur sup-

La reconnaissance des interactions entre traitement, mise à disposition d'informations publiques et protection des données à caractère personnel a entrainé un changement d'approche du droit à la réutilisation des informations publiques. D'un simple « droit individuel à communication des documents sans réutilisation »[8], la directive a permis la mise en œuvre de régimes juridiques distincts : modalités de mise à dispositions des données par les administrations d'une part et modalités d'accès et de réutilisation par des tiers d'autre part. Cette prise en compte, au niveau européen, de la protection des données à caractère personnel dans la mise à disposition d'informations publiques conduisait pourtant à une interdiction de principe de diffusion et de réutilisation des données personnelles contenues au sein d'informations publiques[9].

Pourtant, la nécessité de ne pas considérer la présence de données à caractère personnel comme un frein au développement du mouvement d'*open data,* entendu comme la possibilité de réutiliser des informations publiques[10], a été confirmé par la présence d'un certain nombre d'exceptions dans le texte : recueil du consentement de la personne concernée, anonymisation des données, autorisation par un texte législatif ou encore respect des dispositions de la loi Informatique et Libertés de 1978. Ces différentes exceptions, centrées sur l'exigence de protection des données à caractère personnel, ont surtout été révélatrices de la nécessité croissante à pouvoir réutiliser plus facilement des informations publiques. Un équilibre s'est donc progressivement mis en place entre le besoin de garantir le respect des règles relatives à la protection des données personnelles et le mouvement de transparence administrative fondé sur des possibilités de réutilisation des informations libérées.

---

port, les documents produits ou reçus, dans le cadre de leur mission de service public, par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission ».

(8) C. Castets-Renard, *La transposition de la directive «Psi* 2» et l'ouverture des données publiques, *Dalloz IP/IT*, 2016, p. 6.

(9) L. Cluzel-Métayer, *Les limites de l'open data*, *AJDA*, p. 102.

(10) Pour plus de précisions sur la notion, voir notamment: A. Camus, *La propriété des données publiques*, *RFAP*, n° 167, 2018, p. 479.

A l'heure ou la mise *open data* d'informations publiques devient « un moyen de l'action publique incontournable pour la grande majorité des Etats occidentaux » et que l'Internet apparaît « pour les usagers comme un outil nécessaire au contrôle de l'administration »[11], il est essentiel que les règles relatives à la protection des données à caractère personnel ne constituent pas un frein à ce mouvement, mais contribue au contraire à son développement. L'adoption en France de la loi pour une République numérique en 2016[12] et l'entrée en vigueur du nouveau Règlement européen relatif à la protection des données à caractère personnel en 2018[13] montrent, tout en renouvelant profondément les règles relatives à l'ouvertures des données publiques et à la protection des données, les tensions qui existent parfois entre deux objectifs complémentaires: plus de transparence pour les administrations et respect renouvelé de la vie privée pour les individus.

En France, les acteurs publics ont rapidement pris conscience de la nécessité d'encourager le développement du mouvement d'ouverture des données publiques. Une mission, Etalab, a été créée en 2011 afin de favoriser et de coordonner la récolte de données publiques au sein des différentes administrations de l'Etat. Celle-ci s'inscrit dans un mouvement plus général de développement de la politique publique d'ouverture et prend place au sein d'une « kyrielle de structures *ad hoc* »[14] visant à soutenir la mise en œuvre d'une politique cohérente de mise à disposition des données. Symbole, parmi d'autres, du renouvellement du droit de l'action publique, les modalités de mise à disposition des informations du secteur public reposent désormais sur une ouverture par défaut de l'accès aux informations détenues par l'administration. Codifié en France au Livre III du Code des relations entre le pu-

---

(11) A. Antoine, *Les expériences étrangères d'ouverture de l'accès aux données publiques*, *AJDA*, 2016, p. 81.

(12) Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

(13) Règlement (Ue) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/Ce (Règlement général sur la protection des données).

(14) P. Yolka, *Le droit de l'immatériel public*, *ADJA*, 2017, p. 2047.

blic et l'administration, le principe de réutilisation libre, facile et gratuite des données publiques, tel qu'il est présenté, marque le passage « d'une culture de la détention de l'information à une culture de l'ouverture et de la diffusion »[15].

Le Règlement général européen entré en application le 25 mai 2018 accompagne cette transition en renouvelant profondément les règles relatives à la protection des données à caractère personnel. Également applicables aux personnes publiques, ce texte européen vient modifier les modalités de mise en œuvre de traitement de données à caractère personnel et renforce les obligations qui pèsent sur les responsables de traitement. Bien que de nouvelles contraintes juridiques pèsent sur les personnes publiques, le Règlement n'a pas vocation, sauf pour certaines catégories particulières de données, à limiter les possibilités d'ouverture et de réutilisation des informations publiques. Celui-ci devrait au contraire permettre, à terme, une réutilisation facilitée des informations détenues par les administrations. En effet, le cadre juridique unifié qui est mis en œuvre par le Règlement général européen (§ 2) doit permettre le développement de nouvelles opportunités pour le mouvement d'ouverture des données publiques (§ 3).

2. *Un cadre juridique unifié*

Précédemment contenu au sein de la directive 95/46/CE, le cadre juridique actuelle propre à la protection des données repose sur le recours à un instrument renouvelé, celui du règlement qui ne nécessité pas de loi de transposition pour être directement applicable. Bien qu'une certaine marge de manœuvre soit laissée aux Etats dans l'adaptation de leurs cadres juridiques nationaux par le texte, le recours à cet instrument permet une harmonisation des règles (§ 2.1.) tout en procédant à une responsabilisation des administrations (§ 2.2.).

---

(15) Conseil national du numérique, *Ambition numérique, Pour une politique française et européenne de la transition numérique*, 2015, p. 145.

2.1. *Des règles harmonisées*

Les règles relatives à la protection des données à caractère personnel avaient à l'origine pour but de protéger les individus contre les risques de fichage réalisés par les administrations et par l'Etat. L'adoption d'une loi propre à ce domaine était justifiée à l'époque en France par les révélations du quotidien *Le Monde* relatives au projet dit SAFARI (Système Automatisé pour les Fichiers Administratifs et le Répertoire des individus) d'interconnexion de différents fichiers administratifs nominatifs[16]. La polémique qui a suivi la parution de cet article a permis à cette thématique de faire son apparition dans le débat public et politique. Instrument « très majoritairement aux mains de l'Etat en raison de son coût à l'époque, l'informatique, au travers de cette représentation, a ainsi cristallisé les contestations latentes ou exprimées d'un pouvoir étatique perçu comme menaçant pour la société et l'individu »[17]. Ces différentes conclusions ont permis en 1978 l'adoption d'une législation spécifiquement dédiée à la question de la protection des données à caractère personnel. Mais elles ont également et parallèlement contribué au développement d'un mouvement fondé sur l'idée de transparence de l'action administrative, mouvement confirmé par l'adoption de la loi « CADA » quelques mois plus tard.

Ayant à l'origine pour objet de protéger les individus contre les risques de fichage réalisés par les administrations, les règles relatives à la protection des données personnelles ont été adaptées à la généralisation du recours à l'informatique. Le caractère marchand des données personnelles et l'internationalisation croissante des flux d'informations ont progressivement été pris en compte[18]. Le législateur européen s'est dès lors saisi du sujet avec l'adoption d'une directive visant à assurer la circulation des données dans le respect des droits des individus le 24 octobre 1995[19]. Le système de protection mis en place reposait sur le re-

---

(16) P. BOUCHER, *Safari ou la chasse aux Français*, Le Monde, 21 mars 1974.

(17) N. OCHOA, *Le droit des données personnelles, une police administrative spéciale*, Thèse pour le doctorat en droit présentée et soutenue publiquement le 8 décembre 2014, Université Paris-I Panthéon-Sorbonne, p. 86.

(18) G. DESGENS-PASANAU, *La protection des données personnelles*, 2e éd., LexisNexis, p. 15.

(19) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la

spect, par le responsable de traitement, d'un certain nombre de formalités préalables à la mise en œuvre d'un traitement. Une définition large des données, conservée aujourd'hui, était mise en œuvre puisque celle-ci étaient entendues comme toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement.

Les administrations devaient également respecter ces règles de protection, au même titre que les personnes réutilisant les données libérées, la loi Informatique et Libertés de 1978 mentionnant les autorités publiques parmi les éventuels responsables de traitement. Celles-ci, au même titre que les autres responsables de traitement réutilisant des données libérées, doivent respecter les nouvelles règles mises en place par le Règlement européen et qui repose sur une approche par la conformité des règles de protection. Les personnes publiques appelées à libérer des données en vue d'une éventuelle réutilisation par des tiers sont donc confrontées à une nouvelle réglementation et à de nouvelles contraintes juridiques. Or, celles-ci concernent tous les différents aspects de l'ouverture des données publiques et deux éléments concernent directement les administrations: traitement en amont de données à caractère personnel et mise à disposition en vue d'une éventuelle réutilisation ensuite. Le Règlement général, tout en procédant à l'harmonisation des règles relatives au traitement de données au niveau européen, repose sur une responsabilisation des acteurs concernés et donc, des administrations appelés à traiter des données.

2.2. *Des administrations responsabilisées*

Les autorités publiques sont considérées, à juste titre lorsqu'elles traitent des données, comme des responsables de traitement. Celles-ci doivent donc se conformer aux dispositions protectrices du texte lorsqu'elles collectent des données avant de les mettre à disposition. Une approche par la conformité est à ce titre préconisée par le Règlement européen. Le nouveau cadre européen laisse de côté les formalités préalables en instaurant un cadre juridique qui repose sur la capacité, pour tout re-

---

protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

sponsable de traitement, à pouvoir démontrer à chaque instant le respect de la réglementation. Les autorités publiques, lorsqu'elles mettent en œuvre des traitements de données à caractère personnel, doivent donc être en mesure de démontrer qu'elles agissent conformément à la réglementation. Une spécificité leur est cependant propre: celles-ci sont désormais obligées de désigner un délégué à la protection des données. Simple faculté auparavant, ce recours à un tiers chargé de superviser les traitements réalisés devient obligatoire pour les autorités publiques. Les administrations sont désormais soumises au principe d'*accountability* qui imprègne le nouveau dispositif de protection. Principe général de protection prévu par l'article 24 du texte européen, celui-ci implique que le responsable de traitement mette en œuvre « des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement ». Dès lors, les administrations, au même titre que des opérateurs privés, ont l'obligation de mettre en œuvre des mécanismes qui doivent leur permettre de démontrer à tout moment le respect des règles relatives à la protection des données : analyse d'impact relative à la vie privée[20], pseudonymisation[21], anonymisation ou encore *privacy by design*[22] sont des instruments auxquels les administrations pourront avoir recours pour démontrer leur conformité mais également promouvoir, en amont, un meilleur respect des règles protectrices des données. Cette responsabilisation des administrations lors du traitement de données à caractère personnel, fondée sur une doctrine de protection en amont des données va, *in fine*, permettre une facilitation de la mise en *open data* des informations. Les administrations publiques sont,

(20) Règlement UE (2016/679), article 35.

(21) L'article 25 du Règlement précise ainsi que «le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée».

(22) A. CAVOUKIAN, D. TAPSCOTT, *Who knows: safeguarding your privacy in a networked world*, McGraw-Hill Professional, 1996, p. 5.

pour les besoins de leurs missions, appelés à traiter des données à caractère personnel. Ainsi, « la protection la plus efficiente est celle conçue dès l'origine » et « les bases de données créées par l'administration devraient dès leur origine garantir le respect de la vie privée »[23]. Ces nouveaux mécanismes de protection faciliteront, *in fine*, la réutilisation des informations publiques puisque les données personnelles auront, en amont, fait l'objet d'opérations permettant de respecter la vie privée des individus. Ainsi, plutôt que de représenter un frein au développement de l'*open data*, l'harmonisation des règles de protection au niveau européen constitue surtout une opportunité pour le mouvement d'ouverture des données.

3. *De nouvelles opportunités pour le mouvement d'ouverture des données*

Les données traitées par les autorités publiques doivent désormais prendre en compte un principe de protection des données dès la conception et la mise en œuvre des traitements réalisés. Dès lors, le postulat selon lequel des règles de protection des données renforcées seraient susceptible de freiner la mise en place d'une politique cohérente d'ouverture des données doit être tempéré. Cette harmonisation du cadre juridique au niveau européen doit en effet permettre une réutilisation simplifiée des données pour les tiers (§ 3.1.) tout en contribuant à améliorer la standardisation des données libérées (§ 3.2.).

3.1. *Une réutilisation simplifiée*

Une fois les données collectées et traitées par les administrations publiques, se pose la question de la mise à disposition et de la réutilisation des informations traitées. Le Règlement général européen intègre la mise à disposition dans son champ de protection et assimile celle-ci à un traitement en vertu de l'article 4 du texte. La mise à disposition doit donc respecter les dispositions protectrices du texte et entraîne, pour les administrations, le respect du principe d'*accountability* déjà exposé. Intégrer la question de la mise à disposition des informations directe-

(23) G. Gorce, F. Pillet, *La protection des données personnelles dans l'open data*, cit., p. 25.

ment au sein du Règlement permet une harmonisation des règles qui lui sont applicables. Une telle solution ne peut être que bénéfique au mouvement d'*open data* en raison des difficultés d'interprétation parfois soulevées par les textes nationaux, qu'il s'agisse de la mise à disposition par les administrations ou de la réutilisation des informations par des tiers.

L'ancienne loi CADA de 1978, abrogée et remplacée en 2016 par la loi pour une République numérique[24] présentait le dispositif protecteur propre à la mise à disposition: les documents contenant des données personnelles n'étaient rendus publics qu'après avoir fait l'objet d'un traitement afin d'occulter ces mentions ou de rendre impossible l'identification des personnes qui y sont nommés. Simple dans son principe, le mécanisme prévu à cet article a soulevé un certain nombre d'interrogations sur ses rapports avec les dispositions de la loi Informatique et Libertés. Finalement, le régime de protection contenu dans la loi CADA a été perçu comme un régime de protection autonome, applicable pour les cas ou la publication et la réutilisation n'étaient pas compris comme des traitements de données personnelles[25]. Une solution similaire a été retenue par la loi pour une République numérique. La difficulté à associer ces deux régimes de protection a cependant conduit la CNIL, en France, à publier un pack de conformité précisant la démarche à adopter[26].

Bien que le cadre à respecter ne soit pas tout à fait clarifié, l'harmonisation des règles protectrices par le Règlement européen permet d'entrevoir un début de simplification du régime juridique à appliquer, notamment lorsque celui-ci concerne certaines catégories particulières de données, telles que celles précisées aux articles 9 et 10 du RGPD. Les données à caractère personnel détenues par les administrations sont en effet de nature diverses. Outre la définition générale présentée à l'article 4 du texte, les données à caractère personnel peuvent présenter des spécificités que le texte s'efforce de prendre en compte, telles que

(24) Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

(25) CADA, *Rapport d'activité 2011*, p. 11.

(26) CNIL, *Bilan d'activité 2016*, p. 36.

les données relatives à la santé. Ces spécificités sont également liées, dans certains cas, à la notion d'intérêt public qui est contenue dans le texte européen. La mission d'intérêt public, que le RGPD laisse le soin aux Etats membres de préciser[27], constitue un fondement permettant d'apprécier la licéité des réutilisations de données envisagées. Justifiant la mise en œuvre de certains traitements, cette notion d'intérêt public, appréciée largement, permet aussi de légitimer le traitement ultérieur lorsque celui-ci est réalisée pour des finalités autres que celles prévues lors de la collecte.

Par ailleurs, le considérant 154 du Règlement mentionne explicitement la question des rapports entre *open data* et protection des données personnelles pour les cas de réutilisation des données libérées. Celui-ci insiste sur la nécessité de concilier « la réutilisation des informations du secteur public, d'une part, et le droit à la protection des données à caractère personnel, d'autre part ». La mise en œuvre de traitement de données à caractère personnel obtenues par suite de la mise à disposition par les administrations doit donc respecter les dispositions protectrices renouvelés du Règlement, qu'il s'agisse du consentement préalable renforcé[28] ou de l'obligation d'information qui pèse sur le responsable de traitement, « base du dispositif mis en place puisqu'il constitue le préalable nécessaire à l'exercice des autres droits »[29]. Les obligations qui pèsent sur le responsable de traitement et les droits dont bénéficient les personnes concernées par de tels traitements sont donc renouvelés par le Règlement général. D'application directe au sein des Etats membres, il contribue à la clarification du régime juridique également applicable aux données ayant vocation à être mises à disposition et réutilisées dans le cadre de l'*open data*. Ce renouveau du cadre juridique, complété par l'adoption de la directive du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public[30],

---

(27) Règlement (UE) 2016/679, considérant 10 et 45.

(28) L. MARINO, *Le règlement européen sur la protection des données personnelles: une révolution!*, *La Semaine Juridique*, Edition générale, n°22, p. 6.

(29) M.-C. PONTHOREAU, *La protection des personnes contre les abus de l'informatique*, *RFDA*, 1996, p. 796.

(30) Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant

doit permettre, outre une meilleure protection des informations, de favoriser la standardisation des données traitées et dont le défaut constitue encore aujourd'hui un frein aux mécanismes de l'ouverture des données publiques.

3.2. *Une standardisation encouragée*

L'*open data* constitue, pour les personnes appelées à réutiliser des données libérées, un matériau riche source de nouvelles opportunités. Au-delà de l'accès à l'information qu'elles constituent, les données libérées permettent de « réaliser des services utiles aux consommateurs, aux collectivités, aux marketeurs, aux innovateurs et aux contributeurs citoyens de toutes sortes »[31]. La liberté de réutilisation des données publiques marque la volonté progressive de faciliter la création de nouveaux services par l'accès à des informations auxquelles les individus n'avaient auparavant pas accès. Tel est l'enjeu de l'ouverture des données: outre un objectif de transparence assigné à l'Etat et un renforcement des capacités de l'action publique, l'*open data* apparaît comme un levier pour stimuler l'innovation et la recherche, quels que soit les domaines concernés[32]. L'ouverture des données publiques et les différentes réutilisations qui s'ensuivent doivent permettre à tous de s'approprier et de créer de nouveaux services grâce aux données libérées. La politique d'ouverture des données publiques, fondée sur la possibilité d'accéder et de réutiliser librement et gratuitement l'information, s'inscrit à ce titre dans une perspective large[33].

L'ouverture des données publiques se présente comme un moyen permettant d'accélérer l'activité économique ou encore la croissance sachant que les données constituent un matériau important pour la mise

---

les données ouvertes et la réutilisation des informations du secteur public.

(31) CEREMA, *L'Open Data en collectivité à la lumière des données de mobilités*, Centre d'études et d'expertise sur les risques, l'environnement, la mobilité et l'aménagement, mars 2015, p. 5.

(32) Rapport Commission Open Data en Santé, remis à Madame Marisol Touraine, Ministre des Affaires sociales et de la santé, le 9 juillet 2014.

(33) H. VERDIER, S. VERGNOLLE, *L'Etat et la politique d'ouverture en France*, *AJDA*, 2016, p. 92.

en œuvre de nouveaux services[34]. Mais, outre des problématiques relatives à la protection des données à caractère personnel, la politique d'ouverture se heurte à certaines difficultés pratiques: les administrations ne sont pas toujours prêtes à faire face à ce changement de paradigme fondé sur une culture de l'ouverture de leurs informations. Les données dont disposent les administrations et qui sont sujettes à ouverture ont souvent été collectées dans des formats variés, sans organisation spécifique et sans classement rationalisé. De plus, les administrations, par les différentes missions qu'elles effectuent, disposent d'une quantité importante d'informations qu'elles vont devoir classer, trier et organiser avant de pouvoir les mettre à disposition. Une standardisation des données doit donc être opérée afin que l'*open data* porte réellement ses fruits. En effet, afin de produire des résultats probants, les données mises à disposition devront présenter certains critères de fiabilité et d'exhaustivité.

Généralement incomplètes, désorganisées et contenues au sein de documents aux formats variés, les données dont disposent aujourd'hui les administrations ne font donc pas encore l'objet d'une réelle harmonisation. Malgré d'évidentes contraintes organisationnelles pour les administrations, le développement d'un cadre juridique harmonisé relatif au traitement de données à caractère personnel pourrait pourtant avoir un effet bénéfique. En harmonisant les règles encadrant la collecte de données à caractère personnel, le Règlement général européen pourrait contribuer à la mise en œuvre de traitements rationnalisés dans des formats cohérents et conduisant à la création de données facilement réutilisables. La définition large des données à caractère personnel qui est adoptée permet de corroborer cette affirmation[35]: les administrations vont être amenées, grâce au recours croissant au numérique, à traiter de plus en plus de données à caractère personnel. Celles-ci auront donc vocation à être soumises au dispositif protecteur du Règlement

(34) M. Micheline, *L'ouverture des données publiques dans le contexte de l'open data*, colloque du 3 février 2015, *Lamy Droit de l'immatériel*, 2015, p. 114.

(35) L'article 4 du Règlement (UE) 2016/679 considère qu'une donnée à caractère personnel est « toute information se rapportant à une personne physique identifiée ou identifiable ».

européen et à traiter les données de façon unifiée, facilitant ainsi le processus ultérieur de mise à disposition.
Bien que le Règlement général européen puisse, par le renforcement des règles protectrices mises en œuvre, constituer une contrainte pour les administrations, l'harmonisation des règles qu'il met en œuvre est susceptible d'engendrer des évolutions positives pour le mouvement d'ouverture des données publiques. Outre une responsabilisation des administrations en charge de traiter des données et une meilleure protection des données lors de la réutilisation des informations libérées, le renouveau du cadre juridique protecteur peut contribuer à donner un souffle nouveau au mouvement d'ouverture. Les administrations publiques seront en effet placées sur un pied d'égalité au niveau européen, favorisant le développement de similitudes dans les traitements. La réforme du droit à la protection des données à caractère personnel est intervenue concomitamment à la prise de conscience des bénéfices qu'une ouverture à grande échelle des données publiques pourrait apporter. Cette rénovation de la législation pourra dès lors et après un premier temps d'adaptation, servir d'impulsion au mouvement d'ouverture des données publiques, afin que celui-ci se propage de manière efficace et pérenne. Une telle dynamique serait alors semblable à celle ayant eu lieu en 1978 et ayant donné naissance à un cadre protecteur des données d'une part et à un mouvement de transparence de l'action administrative d'autre part.