"Autodétermination informationnelle, droit à la vie privée, right to privacy : quel noyau pour la protection des données personnelles ? L'apport du droit comparé : Union européenne, Allemagne, France, Royaume-Uni"

Christina Koumpli

▶ **To cite this version:**

Christina Koumpli. "Autodétermination informationnelle, droit à la vie privée, right to privacy : quel noyau pour la protection des données personnelles ? L'apport du droit comparé : Union européenne, Allemagne, France, Royaume-Uni". Pauline Türk (dir.), Droit et libertés numériques catégorie ou génération de droits fondamentaux, Actes de colloque, Collection, Droit et Société, LGDJ, 2024, LGDJ, inPress, Droit et société. hal-04673482

HAL Id: hal-04673482
https://hal.science/hal-04673482v1

Submitted on 20 Aug 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Copyright

« Autodétermination informationnelle, droit à la vie privée, *right to privacy* : quel noyau pour la protection des données personnelles ?
L'apport du droit comparé : Union européenne, Allemagne, France, Royaume-Uni »

Christina KOUMPLI

Maître de conférences en droit public
Avignon Université, Chercheur LBNC EA3788

Depuis l'entrée en vigueur du Traité de Lisbonne, l'article 16 du Traité sur le fonctionnement de l'Union européenne (TFUE) ainsi que l'article 8 de la Charte des droits fondamentaux de l'Union européenne (CDFUE) consacrent expressément que « *1. Toute personne a droit à la protection des données à caractère personnel la concernant* ». Il est toutefois manifeste que le caractère fondamental de la protection des données à caractère personnel[1] ne persuade pas la doctrine[2]. En effet, cela continue de l'interroger, et sans doute très justement dans la mesure où l'on ne sait pas exactement ce qui est vraiment protégé par ce droit. Le (droit) fondamental étant en Droit ce qui justifie des limites portées à d'autres droits fondamentaux et ce qui ne peut supporter plus de limitations que celles qui s'arrêtent aux contours de son noyau essentiel (« limite des limites »)[3], l'interrogation reste entière quant à la question de savoir ce qui est *propre* à la protection des données personnelles, ce qui la justifie, et ce qui est attentatoire à son contenu essentiel.

La question est importante si l'on songe à l'injonction faite par l'article 52§1 de la CDFUE[4] de connaître le « contenu essentiel » des droits fondamentaux prévus par la Charte au moment de les interpréter. Elle l'est encore plus lorsque l'on constate que faute de connaître la nature de ce droit, les juges se résignent soit au rappel (au pire), soit à la vérification (au mieux) des conditions et principes prévus par le cadre législatif en vigueur, soit (encore pire) à l'exigence de garanties techniques supplémentaires[5], ce qui ne fait que déplacer le fond du problème (y a-t-il ou non atteinte et à quoi ?).

En faisant comme si le droit fondamental ***à la*** protection des données à caractère personnel trouvait satisfaction dans le droit ***de la*** protection des données personnelles, tel que prévu par le législateur, la *neutralisation* est non seulement flagrante ; elle est surtout très problématique. En effet, un droit fondamental ne peut se diluer dans une législation qui le matérialise (à moins que celle-ci ait acquis valeur supra-législative), puisque, dans ce cas, la conformité, par rapport au droit fondamental, de la loi et de ses modifications ultérieures ne pourrait plus être contrôlée.

Il convient donc de sortir le droit à la protection des données à caractère personnel d'un raisonnement circulaire visant à légitimer tout traitement de données personnelles par une

---

[1] Les expressions « données personnelles » et « données à caractère personnel » seront utilisées de façon interchangeable.
[2] v. L. Cluzel-Métayer, dans cet ouvrage….(à compléter avant la publication)
[3] O. Pfersmann, *in* Louis Favoreu, *Droit des libertés fondamentales*, 7e édition, Dalloz, Coll. Précis, p.91
[4] CDFUE, Article 51 – Portée et interprétation des droits et des principes :
« *1. Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés* ».
[5] Ex. Cons. const., n° 2020-800 DC du 11 mai 2020.

satisfaction des conditions légales de mise en place de celui-ci. Ce n'est que de cette façon qu'il sera possible de préciser le caractère « fondamental » de ce droit afin de mettre fin à l'interrogation sur son existence et ses propriétés. Ceci alors que les technologies actuelles rendent déjà obsolète le cadre légal de la protection des données personnelles[6]. À cette fin, nous proposons une réflexion en trois temps :

I) en premier lieu, il s'agira de rappeler qu'en droit de l'UE, le sens du droit fondamental à la protection des données à caractère personnel reste ouvert à des interprétations discordantes ;

II) ensuite, nous démontrerons en quoi le recours à des concepts nationaux tels que le droit au respect de la vie privée, le *right to privacy* et le droit à l'autodétermination informationnelle peuvent donner une direction interprétative intéressante mais pas suffisante au droit de la protection des données à caractère personnel ;

III) enfin, il conviendra de souligner la nécessité de dépasser le rattachement aux individus du droit à la protection des données personnelles afin que ce droit puisse prendre en compte les enjeux collectifs du traitement des données personnelles en correspondance avec les risques actuels lesquels dépassent le cadre personnel.

I- UN DROIT FONDAMENTAL EN QUETE DE SIGNIFICATION AU NIVEAU DE L'UNION EUROPEENNE

Afin de traiter cette question, nous suivrons un raisonnement en trois étapes. Il s'agira, tout d'abord, d'observer que l'UE détient désormais un monopole en matière de protection des données personnelles (a). Or, du fait des caractéristiques et besoins fonctionnels propres à cet ordre juridique, cette protection a un caractère bi-fonctionnel, étant donné qu'elle vise non seulement à garantir les libertés individuelles mais surtout à permettre la réalisation d'un marché commun (b). Néanmoins, la fondamentalisation européenne dont la protection des données personnelles fait preuve pourrait correspondre à une protection affaiblie (c).

a) Le monopole de l'UE en termes de protection des données personnelles

Avec l'entrée en vigueur du Traité de Lisbonne, il s'est produit une « montée normative »[7] de la protection des données personnelles au sein de l'UE. En d'autres termes, c'est à ce moment que l'ordre juridique européen s'est attribué le monopole de la conception et de l'organisation de la protection des données personnelles traitées au sein des États membres.

[6] Axel Voss, « EU must overhaul flaship data protection laws, says a 'father' of policy », *Financial Times*, 3 mars 2021 ; Thomas Zerdick, « Is the future of privacy synthetic ? », 14 juillet 2021, disponible en ligne sur le site du *European Data Protection Supervisor* (EDPS) [consulté le 22/02/2022 : https://edps.europa.eu/press-publications/press-news/blog/future-privacy-synthetic_en]. Voir aussi la dernière partie de la présente contribution sur le concept de « *synthetic data* ».

[7] Nous entendons par « montée normative » la consécration progressive d'une valeur supra-législative au droit à la protection des données à caractère personnel par différents moyens (inscription dans les Constitutions nationales, consécration par les juges constitutionnels, inscription dans un Traité, usage du droit pour invalider une norme juridique de l'ordre juridique, etc.) en ce sens v. Christina Koumpli, *Les données personnelles sensibles : une contribution à la protection du droit fondamental à la protection des données à caractère personnel. Étude comparée : Union européenne, Allemagne, France, Grèce, Royaume-Uni*, , Pedone, 2022], pp. 22-24 et 142 et s.

En effet, le Traité de Lisbonne a tout d'abord accordé une valeur contraignante à la CDFUE (art. 6§1, TUE) qui a consacré, pour la première fois au niveau supranational[8], un droit fondamental spécifique (art. 8, CDFUE) sans que celui-ci n'ait d'équivalent dans la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales (CEDH)[9]. Même s'il s'agissait initialement d'une réaffirmation de droits existants, dans le cadre de la démarche consistant à marquer une « *transformation de l'essence même de l'Europe... d'un marché commun, d'une union économique...* [vers] *une union politique et d'une communauté de valeurs* »[10], l'élaboration d'une Charte qui n'aurait pas fait allusion à des droits contemporains n'était pas envisageable en 2000[11]. C'est dans cet état d'esprit que la protection des données personnelles s'est autonomisée du droit au respect de la vie privée, selon le *Praesidium* de la Convention qui a élaboré la Charte. Cependant, la « fondamentalisation » de la protection des données personnelles à travers l'article 8 de la CDFUE va bien au-delà de déclarations à caractère symbolique et d'ordre politique. Elle a une véritable portée juridique : la protection affirmée par cette disposition peut être considérée comme fondant un droit qui ne relève plus de « droits correspondants » dans la CEDH, ni de « traditions constitutionnelles communes des États membres » (art. 52, § 3 et 4, CDFUE). L'article 8 de la CDFUE a ainsi ouvert une brèche pour l'élaboration d'une conception autonome - par rapport à celle retenue par la CEDH et les États membres – et propre à l'UE du droit à la protection des données à caractère personnel.

Cette ouverture est soutenue par l'article 16 du TFUE[12] qui prévoit une obligation de concrétisation pesant sur le législateur de l'Union[13]. Le sens et la portée de ce nouveau droit fondamental pouvaient ainsi être définis par le législateur de l'Union; ce qui ne tarda pas à arriver, avec l'adoption du « Paquet européen de protection des données personnelles » contenant le Règlement général sur la protection des données (RGPD)[14] et la Directive « Police-Justice »[15].

Or, si l'article 8 de la CDFUE permet symboliquement de consacrer la « fondamentalisation » de ce droit, l'article 16 du TFUE est en réalité la disposition qui permet d'organiser la mise en place du monopole européen en matière de concrétisation de celui-ci. En effet, avec le Traité

---

[8] Guy Braibant, *La Charte des droits fondamentaux de l'Union européenne. Témoignage et commentaires*, Paris, Ed. du Seuil, 2001, p. 71.

[9] Mihaela Anca Ailincai, « Différents standards européens de protection des données ? A propos du droit de l'Union européenne et du droit du Conseil de l'Europe », colloque Rennes, Alexandra Bensamoun et Brunessen Bertrand (dir.), *Le Règlement général sur la protection des données. Aspects institutionnels et matériels*, 16 novembre 2018 ; disponible en ligne sur : researchgate.net

[10] G. Braibant, *op. cit.*, p. 17.

[11] *Ibidem*, p. 47.

[12] Hielke Hijmans, *The European Union as guardian of Internet Privacy. The story of article 16 TFUE*, Springer, 2016, 604 p.

[13] L'objet de l'article 16 du TFUE n'émerge pas avec le Traité de Lisbonne mais ce dernier modifie radicalement le contenu et la portée de l'article 286 TCE qui le précédait. Pour une analyse approfondie sur le sujet, voir Christina Koumpli, thèse, *op. cit.*, pp. 140 et s.

[14] 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 (dit « Règlement général sur la protection des données » ou RGPD).

[15] Au RGPD s'ajoute l'autre volet du « Paquet européen de protection des données personnelles », à savoir la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

d'Amsterdam, il s'agissait de donner un effet horizontal à un instrument juridique d'effet vertical (Directive 95/46/CE). Désormais, il s'agit d'offrir au législateur européen un fondement exprès pour légiférer en la matière, dépassant ainsi les dispositions de la Charte et de la jurisprudence de la Cour de justice de l'Union européenne (CJUE) réitérant l'absence de compétence propre de l'Union en matière de garantie des droits fondamentaux. Ainsi, si la Charte ne change rien quant au partage des compétences entre l'Union et les États membres en matière de protection des données personnelles, l'article 16 du TFUE attribue cependant à l'Union une compétence pour légiférer.

« Le législateur [était] ainsi désormais contraint à l'excellence, grâce à la constitutionnalisation du droit et à la vigilance du juge »[16]. Son office a confirmé le caractère de droit fondamental de l'article 8 de la CDFUE puisque le juge de Luxembourg a invalidé des normes nationales[17] et européennes[18] en application de cette disposition ; surtout il n'a pas hésité à faire trembler l'échiquier international[19] du droit du numérique en mettant en cause l'ordre juridique sur la base duquel se développent les géants du numérique.

Ainsi, d'une part, le droit de l'UE a contribué à l'acquisition par la protection des données personnelles d'un caractère de droit fondamental; d'autre part, et dans le même temps, il s'est attribué la compétence de garantie de ce nouveau droit fondamental sur la base du triple fondement du Traité de Lisbonne, de la CDFUE et de la jurisprudence de la CJUE[20]. Cette situation empêche, en principe, toute fissure de l'autonomie de l'ordre juridique de l'Union[21]-[22] en la matière.

b) Une norme à caractère bi-fonctionnel

Dans un deuxième temps, il convient de remarquer que ce monopole de protection des données par l'UE est une grande avancée, à la fois interne à l'UE en raison de l'harmonisation maximale dont le RGPD pose les conditions, mais aussi externe à celle-ci au regard de l'extraterritorialité attribuée à ce texte[23] qui place l'Union en position d'acteur dominant sur la scène de l'économie numérique mondiale à travers la vision d'un numérique éthique qu'elle entend imposer.

Néanmoins, il convient aussi de remarquer que la motivation de l'ordre juridique de l'UE à l'égard de la protection des données n'émane pas de seules préoccupations relatives à la

---

[16] Sylvie Peyrou, « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la CJUE », *in* Romain Tinière, Claire Vial (dir.), *La protection des droits fondamentaux dans l'Union européenne. Entre évolution et permanence*, Bruxelles, Bruylant, coll. « Colloques », 1re éd., 2015, p. 215.

[17] Par exemple : CJUE, 9 mars 2010, *Commission c/ Allemagne*, aff. C-518/07 ; CJUE, 16 octobre 2012, *Commission c/Autriche*, aff. C-614/10 ; CJUE, 8 avril 2014, *Commission c/ Hongrie*, aff. C-288/12.

[18] Par exemple : CJUE, 8 avril 2014, *Digital Rights Ireland Ltd c/ Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.*, aff. C-293/12.

[19] Par exemple : CJUE (Gr. Ch.), 6 octobre 2015, *Maximillian Schrems contre Data Protection Commissioner*, aff. C-362/14 (invalidation du *Privacy Schield*).

[20] Sylvie Peyrou, *op. cit.*, pp. 213 et s.

[21] *Ibidem*

[22] Il convient de signaler le risque lié à ce monopole qui consisterait à ne plus pouvoir apprécier la validité du RGPD, si ce dernier était désormais abordé comme la réalisation suffisante (et parfaite) du droit primaire et non comme une simple concrétisation de ce dernier. Dans un tel schéma, l'article 8 CDFUE ne pourrait plus vraiment jouer son rôle de droit fondamental (au sens d'une permission d'agir dont la violation par un acte législatif pourrait conduire à la sanction de l'organe de contrôle compétent).

[23] Non seulement à travers l'extraterritorialité mais aussi par le biais de divers mécanismes de légalisation des transferts hors UE tels que les décisions d'adéquation, les « Binding Corporate Rules », les Clauses Contractuelles Types, les codes de conduite, ou encore les labélisations.

protection des libertés individuelles, comme cela est le cas du Conseil de l'Europe. Ici, la protection des données à caractère personnel est une condition à la réalisation du projet d'intégration européenne et à la compétitivité de l'Union sur le plan international. C'est en ce sens que nous considérons que le droit à la protection des données personnelles dans le cadre de l'ordre juridique de l'UE dispose d'un caractère bi-fonctionnel. Le cadre protecteur des données personnelles vise, en effet, à garantir la libre circulation des données personnelles en tant que condition essentielle de la réalisation de l'intégration européenne, tout en protégeant les droits fondamentaux des personnes concernées par le traitement de leurs données[24].

Cette conciliation inhérente à la protection des données personnelles au sein de l'UE résulte de l'observation de plusieurs éléments. Tout d'abord, au regard de la Directive 95/46/CE (qui constitue l'ancêtre du RGPD et donc, d'une certaine façon, son ADN) : en effet, c'est l'objectif de rapprochement des législations nationales protectrices des données personnelles en vue de l'établissement d'un marché commun de la Communauté européenne qui a conduit à l'adoption d'un cadre juridique visant à concilier la nécessité d'une libre circulation des données avec une protection tout aussi indispensable des droits fondamentaux[25], cadre que le RGPD a renouvelé et accentué. En outre, la comparaison des objectifs de la Convention 108[26] et de la Directive 95/46/CE (et désormais du RGPD) est assez révélatrice d'une différence de finalité de la protection dans les deux ordres juridiques européens. Ce qui distingue ces deux textes est une préférence pour l'une ou l'autre priorité : marché/droits fondamentaux. Le « coefficient » de protection dans le texte du Conseil de l'Europe penche du côté des libertés des personnes physiques[27]. Par ailleurs, il convient de rappeler qu'en l'absence de compétence générale de l'UE pour édicter des normes en matière de droits fondamentaux, ni à l'époque de la Directive 95/46/CE ni au moment de l'entrée en vigueur du RGPD, la *protection* des données à caractère personnel ne peut être son seul objet d'action. Ainsi, cette protection fait partie du respect des droits fondamentaux dont la Communauté (CEE) puis l'Union européenne font ~~(ont fait ?)~~

[24] Pour une analyse approfondie du droit positif de l'UE laissant apparaître le caractère bi-fonctionnel de la protection des données au sein de l'UE, voir Christina Koumpli, thèse, *op. cit.*, pp. 121-181.

[25] La nécessité d'harmoniser les législations nationales afin de permettre la libre circulation des données personnelles au sein de la Communauté européenne, qui participe de la réalisation d'un marché commun, constitue le fondement de la Directive 95/46/CE ; ce que la CJUE n'a pas ignoré. Voir, par exemple : CJCE, 20 mai 2003, *Österreichischer Rundfunk* (cons. 39-70).

[26] Conseil de l'Europe, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, 28.I.1981. (dite « Convention 108 »)

[27] En effet, la Convention 108 a été adoptée « considérant qu'il est souhaitable d'étendre la protection des droits et des libertés fondamentales de chacun, notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés » (préambule). Par ailleurs, son article 1er précise : « Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (protection des données) ».

L'article 1er du RGPD (objet et objectifs) pose quant à lui la conciliation comme axe d'interprétation :

« 1. Le présent règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données.

2. Le présent règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel.

3. La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ».

preuve depuis plusieurs décennies[28] ; et dont la valeur la CDFUE consacre afin qu'elle soit respectée dans la mise en place des politiques permettant la réalisation de l'objectif d'intégration européenne.

Enfin, la preuve la plus probante de ce caractère bi-fonctionnel du droit à la protection des données personnelles est la place attribuée à cette protection dans le TFUE. Alors que l'on peut croire, à la suite d'une lecture hâtive de l'article 16 du TFUE, que cette disposition accorde une compétence propre à l'UE en matière de protection des données personnelles, l'appartenance de l'article 16 TFUE au Titre II intitulé « Dispositions d'application générale » (qui suit celui dédié aux « Catégories et compétences de l'Union »), laisse entendre le caractère primordial accordé à cette reconnaissance et à ce transfert de pouvoirs pour l'UE[29].

Sans une libre circulation des données personnelles, l'Union ne pourrait correctement fonctionner. Ainsi, la disposition contenue dans l'article 16 du TFUE a une fonction téléologique d'instrumentalisation « presque involontaire » de la protection des données personnelles par l'UE : il s'agit d'encadrer une situation nécessaire à l'Union, c'est-à-dire la libre circulation des données qui est un préalable à la réalisation du projet d'intégration européenne dans son ensemble.

b) Un droit qui affaiblit potentiellement la protection

En troisième lieu, alors que l'on peut se féliciter de ce « *Brussels effect* »[30] bénéfique à l'image de l'UE - mais aussi aux libertés numériques des citoyens européens indépendamment de leur localisation sur la planète à un instant *t* - il convient néanmoins de souligner l'interrogation que soulève ce monopole et cette dépendance à l'UE de la libre circulation des données à caractère personnel.

On peut alors se demander : n'a-t-on pas attribué une valeur de droit fondamental à un cadre protecteur qui *ab initio* a une portée réduite en termes des garanties des citoyens européens ?

Plus précisément, notre hypothèse d'une protection affaiblie repose sur la réflexion suivante : la protection des droits fondamentaux résultant de l'aménagement de leur garantie en vue de privilégier l'objectif prioritaire de réalisation d'un marché commun serait, selon nous, le résultat d'une soustraction entre une « plus-value », les objectifs communautaires, et une « moins-value », la garantie des droits fondamentaux. En effet, pour l'Union européenne, la limitation des droits fondamentaux impliquée par un traitement informatique des données personnelles est envisagée comme nécessaire en vue de la réalisation du marché commun mais elle doit cependant être encadrée par certaines règles protectrices de la personne. Cette conciliation est inhérente à la conception de la protection des données personnelles dans l'ordre juridique de l'Union. C'est en ce sens que l'on soutient l'idée selon laquelle l'article 8 de la CDFUE pourrait impliquer une protection affaiblie par rapport à une protection monofonctionnelle (telle celle

[28] En ce sens (*respect* ne veut pas dire *compétence), voir* V. Skouris, « La protection des droits fondamentaux dans l'Union européenne dans la perspective de l'adoption d'une constitution européenne », *in* L. Serena Rossi (dir.), *Vers une nouvelle architecture de l'Union européenne*, Bruxelles, Bruylant, 2004, p. 239 : « *Pourtant, l'énumération des droits de la Charte ne signifie pas que l'Union devient compétente dans les matières couvertes par ces droits, mais simplement qu'elle doit les respecter* ».

[29] Inutile de remarquer qu'il fait partie des rares droits de la Charte à bénéficier d'un statut aussi privilégié.

[30] A. Bradford, *The Brussels effect. How the European Union Rules the World*, 2020, Oxford University Press, 424 p.

de la vie privée, par exemple - malgré le fait que ce concept n'est plus pertinent face aux dangers actuels du numérique pour les libertés, comme il sera expliqué plus loin).

À défaut de savoir en quoi consiste vraiment la « protection » prévue par l'article 8 de la CDFUE et faute de comprendre son articulation avec l'article 16 du TFUE qui a donné naissance au RGPD, une logique circulaire s'installe Un « reflet miroir » entre la norme de droit primaire et la norme de droit dérivé peut se développer, en ce sens qu'à défaut de pouvoir appréhender son objet, on s'abritera derrière les dispositions du droit dérivé en la matière. Du fait d'une apparition historique inversée des normes[31], au lieu de chercher à interpréter et concrétiser le droit fondamental dans tel ou tel cas, le juge peut choisir la facilité en lisant dans le droit fondamental un « concentré » de la « loi spéciale » de droit dérivé (ici le RGPD). Or, prenant le cas d'école d'un juge qui aurait à se prononcer sur la conformité à l'article 8 de la CDFUE d'un traitement (mis en place par un acte étatique/européen/ou d'une entreprise), il y a alors de très fortes chances que cette conformité ne soit pas refusée si le responsable du traitement en question a mis en œuvre différentes mesures d'*accountability* tel que le prévoit le RGPD (mesures de « *privacy by design* », désignation d'un « *data protection officer* », élaboration de « *privacy impact assessments* », etc.).

Est-ce cela la « protection », objet ~~(de permission)~~ du droit fondamental ? Quelle marge reste-t-il aujourd'hui pour un contrôle du RGPD par rapport à la Charte ? Si la fondamentalisation de la protection des données par l'article 8 de la CDFUE et 16 TFUE fait « monter » le RGPD parmi les normes de référence du contrôle des traitements, cela pourrait conduire à exclure ce texte d'un contrôle.

II. LES APPRENTISSAGES NATIONAUX ET LEURS LIMITES

Les lignes précédentes ont permis d'analyser une situation contestable, celle ~~Devant cette situation contestable~~ d'un droit fondamental potentiellement réducteur des libertés fondamentales en raison de la conciliation de valeurs opposées qu'il comporte ; contestable aussi du fait que la protection des données pourrait être interprétée au travers du seul prisme de sa concrétisation législative à travers le RGPD (comme si le droit fondamental se réduisait à une permission accordée à son titulaire de faire respecter le RGPD). Il convient désormais de porter notre regard sur les ordres juridiques nationaux qui ont consacré des concepts pertinents sur le sujet.

Le rattachement au droit au respect de la vie privée (France), au *right to privacy* (Royaume-Uni) (a), ou au droit à l'autodétermination informationnelle (Allemagne) (b) sont des solutions particulièrement intéressantes en ce qu'elles se rapportent à un dénominateur commun, à savoir une interprétation « anthropocentrée » de l'article 8 de la CDFUE qui pourrait être perçue en tant que tradition constitutionnelle commune (c). Chacune présente toutefois quelques limites qu'il conviendra d'exposer.

a) Le rattachement au droit à la vie privée / *right to privacy* et leurs limites

Les droits français et britannique éclairent le sens du droit fondamental à la protection des données à caractère personnel à travers son rattachement supra-législatif à un droit constitutionnel générique : le respect de la vie privée. Il ne s'agit pas ici, bien évidemment, de faire un amalgame entre respect de la vie privée et *privacy*, le rapprochement des deux notions

[31] Directive 95/46CE d'abord, puis CDFUE, puis TFUE.

pouvant uniquement permettre la considération de problématiques de droit similaires bien que l'on se réfère à des ordres juridiques structurellement différents[32]. Brièvement, rappelons que le *right to privacy* au Royaume-Uni a été construit au regard de la notion de « propriété négative » (au sens d'un espace auquel l'accès n'est pas autorisé par le biais des notions de « *tresspass to land* » et « *breach of confidence* »)[33]. Cependant, une approche historico-juridique de la protection des données à caractère personnel au Royaume-Uni permet de révéler que, surtout depuis le *Human Rights Act* et la jurisprudence de la Cour de Strasbourg relative à l'article 8 de la CEDH, la protection des données à caractère personnel a acquis des aspects relevant d'une garantie positive. En effet, la protection des données à caractère personnel était, et est encore, interprétée comme un acte positif du législateur permettant de mieux garantir le *right to privacy*[34]. Cette situation juridique rejoint finalement le droit français, sachant que le Conseil constitutionnel a abordé la loi informatique et libertés (sa logique et son vocabulaire) comme une garantie légale d'une exigence constitutionnelle, désormais cristallisée au nom du droit au respect de la vie privée dégagée à partir de l'article 2 de la Déclaration des droits de l'homme et du citoyen (DDHC) et plus spécifiquement de la notion de « liberté ».

Les concepts de « *right to privacy* » et le « droit au respect de la vie privée » permettent de donner une direction au droit à la protection des données à caractère personnel ou bien une option (parmi d'autres) de lecture face à l'ambiguïté de l'article 8 de la CDFUE. Cette interprétation permettrait, en tout état de cause, d'axer autour de la personne la concrétisation de la protection (plutôt qu'autour de la libre circulation des données conformément aux dispositions du RGPD).

Ce rapprochement entre protection des données personnelles et droit au respect de la vie privée est d'ailleurs plébiscité non seulement par la jurisprudence mais aussi par la doctrine. Sans le faire de manière exhaustive, on peut aussi de mentionner la jurisprudence de la CJUE dans laquelle le droit au respect de la vie privée et le droit à la protection des données personnelles sont utilisés l'un aux côtés de l'autre, comme si ce dernier complétait les insuffisances du premier et que le premier apportait une direction nécessaire au second afin que celui-ci ne prenne pas de voies discutables[35].

Telle est l'opinion d'une partie de la doctrine. Par exemple, Yves Poulet et Antoinette Rouvroy considèrent que l'autonomisation du droit à la protection des données personnelles (par rapport au droit à la vie privée) risque de rendre inintelligibles les fondements des régimes de protection des données personnelles (dignité et autonomie) et plus difficile la tâche du législateur lorsqu'il aura à évaluer et à revoir les instruments de protection au vu des évolutions sociopolitiques et

[32] J-L. Halpérin, « Protection de la vie privée et *privacy* : deux traditions juridiques différentes ? », *Les nouveaux cahiers du Conseil constitutionnel*, dossier : Vie privée, n° 48, juin 2015, pp. 59-68.
[33] P. Kayser, *La protection de la vie privée*, Aix-en-Provence, PUAM, 2e éd., 1990, pp. 62-63 ; D. Feldman, *Civil Liberties and Human Rights in England and Wales*, Oxford University Press, 2e éd., 2002, p. 544.
[34] Pour un résumé de l'historique de cette évolution, voir C. Koumpli, thèse, *op. cit.*, pp. 67 -82.
[35] L'influence de la Cour européenne des droits de l'Homme en tant qu'interprète légitime des droits fondamentaux sur le plan du droit international régional peut aussi contribuer à ce rattachement (par reconnaissance donc de son rôle).

technologiques de la société de l'information[36], dans sa dimension globale et au seuil de « l'ère d'intelligence ambiante »[37].

En revanche, des auteurs comme Paul de Hert et Serge Gutwirth refusent l'emploi interchangeable des deux notions en expliquant qu'il existe d'importantes différences entre les deux en termes de champ d'application, d'objectifs et de contenu. La protection des données à caractère personnel, d'après eux, protège explicitement des principes qui n'intègrent pas le noyau de la vie privée (ou de la *privacy*) telles que l'exigence d'un traitement loyal des données, le consentement préalable au traitement et la non-discrimination[38]. Ainsi, ils considèrent que « (...) *la reconnaissance d'un droit séparé de protection des données personnelles, aux côtés du droit au respect de la vie privée (privacy), est plus respectueuse de l'histoire constitutionnelle européenne* »[39] .

Les efforts de la doctrine en vue de clarifier le rapport entre respect de la vie privée et protection des données à caractère personnel sont notables dans plusieurs travaux[40] alors qu'il serait, à notre sens, plus pertinent que jamais de relire et de donner une force contraignante à l'article 1er de la loi informatique et libertés de 1978 dans sa rédaction initiale :

> « *L'informatique doit être* ***au service de chaque citoyen***. (…). *Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

Le droit au respect de la vie privée étant la notion la plus perceptible de la liste ainsi mentionnée, elle a monopolisé tout le débat en éloignant la réflexion de l'essentiel, qui est en réalité davantage un danger collectif[41] qu'individuel, déjà à l'époque de la promulgation de cette loi.

Alors qu'il est désormais évident que le pouvoir de connaissance[42] permis par le traitement des données personnelles - cette connaissance sur mesure qui permet de « calculer l'incalculable » comme l'écrit Alain Supiot[43] - dépasse largement la problématique du respect de la vie privée et de la *privacy,* et alors que le constat semble aujourd'hui unanime sur le fait qu'un rattachement de la protection des données à la vie privée revient à « *mettre du nouveau vin dans*

---

[36] Y. Poullet, Antoinette Rouvroy, « Le droit à l'autodétermination informationnelle », *in* K. Benyekhlef, P. Trudel, *État de droit et virtualité*, Montréal, Thémis, 2009, pp. 210, 213, 218-219.

[37] A. Rouvroy, « Privacy, Data protection and the Unprecedented Challenges of Ambient Intelligence », *Studies in Ethics, Law and Technology*, Berkeley Electronic Press, 2, 1, 2008, pp. 1-54.

[38] Paul de Hert, Serge Gutwirth, « Data protection in the case law of Strasbourg and Luxembourg: Constitutionalisation in action », *in* Serge Gutwirth, Yves Poullet *et alii*, *Reinventing data protection?*, Springer, 2009, p. 9.

[39] *Ibidem*, p. 10 (nous traduisons : "*We believe that the recognition of a separate right to data protection, next to privacy, to be more respectful to the European constitutional history*").

[40] Gloria Gonzalez-Fuster, « The Emergence of Personal Data Protection as a Fundamental Right of the EU », *Springer, Law, Governance and Technology Series*, vol. 16, 2014; Paul de Hert, Serge Gutwirth, *op. cit.*, p. 10 ; Yves Poullet, Antoinette Rouvroy, *op. cit.*, p. 210 ; Antoinette Rouvroy, *op. cit.*, pp. 1-54.

[41] v. la dernière partie de la présente contribution.

[42] « (…) *l'information représente pour ceux qui la détiennent un pouvoir vis-à-vis de ceux sur lesquels l'information est détenue. Celui qui détient l'information sur autrui peut adapter sa décision en fonction de la connaissance que l'information collectée et traitée lui donne d'autrui. Il prévoit son attitude et peut donc répondre à sa demande ou influencer celle-ci », Yves Poullet, Jean-François Henrot, « La protection des données (à caractère personnel) à l'heure de l'Internet* », *in* Jacques Laffineur (dir.), *Protection du consommateur, pratiques commerciales* et T.I.C., collection CUP - Commission Université Palais, volume 109, 2009, p. 199

[43] Alain Supiot, « Calculer l'incalculable : la doctrine Law and Economics » (Chapitre 7), *in* Alain Supiot, *La gouvernance par les nombres. Cours au Collège de France (2012-2014)*, Paris, Fayard, 2015, pp. 183-213.

de vieilles bouteilles »[44], ce rapprochement est néanmoins toujours dominant (peut-être parce qu'il permet la translation et la communication avec d'autres ordres juridiques comme celui des États-Unis).

Or, il est urgent que la recherche pluridisciplinaire réussisse à démontrer comment le traitement automatisé des données personnelles peut porter atteinte aux éléments énoncés à l'article 1er de la loi informatique et libertés de 1978 ; à savoir dans quels cas et dans quelle mesure la vie privée, mais également l'identité humaine, les droits de l'homme et les libertés individuelles ou publiques sont mis en danger par le traitement de données à caractère personnel.

Pour l'instant, de telles réflexions sont absentes, à la seule exception du rapport du Défenseur des droits sur la prévention de l'automatisation des discriminations par les algorithmes[45], et des commentaires à l'issue du scandale de *Cambridge Analytica* qui fait planer une crainte quant à l'impact néfaste du traitement des données personnelles sur la démocratie.

b) Le rattachement à l'autodétermination informationnelle et ses limites

L'apport du droit allemand sur cette question se rapporte à la notion, particulièrement séduisante par son caractère éloquent et impérissable, d'autodétermination informationnelle (*Das Recht auf informationelle Selbstbestimmung*). Le Conseil d'État, dans une étude de 2014 intitulée *Le numérique et les droits fondamentaux*[46], et un rapport de l'Assemblée nationale intitulé *Numérique et libertés : un nouvel âge démocratique* de 2015[47] ont fait l'éloge de l'utilité de ce droit d'origine germanique face au risque de contractualisation du droit au respect de la vie privée. L'article 54 de loi pour une République numérique lui a ainsi consacré une place privilégiée (sans toutefois le nommer expressément) à travers l'ajout d'un alinéa à l'article 1er de la loi informatique et libertés. Il a donc désormais valeur législative dans l'ordre juridique français[48].

Mais ce droit est-il aussi pertinent que cela a pu être affirmé ?[49] Pourrait-il permettre une interprétation appropriée du droit à la protection des données à caractère personnel face aux risques des technologies numériques actuelles ? L'autodétermination informationnelle, qui n'est pas soluble dans les concepts de vie privée ou de *privacy*, sans doute permet de réfléchir un peu plus sur les risques réels du traitement des données personnelles qui sont de loin bien plus nombreux que l'atteinte à la vie privée. En effet, le droit au respect de la vie privée a un

---

[44] Spiros Simitis, « Les données sensibles en quête d'un régime juridique, *in* Conseil de l'Europe, *Problèmes législatifs de la protection des données*, Athènes, Conférence Internationale, 18-20 novembre 1987, Conseil de l'Europe, Ministère de la Justice de Grèce, Athènes – Komotiní, Sakkoulas, 1991, p. 289.

[45] Défenseur des droits et CNIL, *Algorithmes : prévenir l'automatisation des discriminations*, Rapport, 2020, 11 p.

[46] Conseil d'État, *Le numérique et les droits fondamentaux*, Étude annuelle 2014, Paris, La Documentation française, spéc. pp. 267 et s.

[47] Assemblée nationale, *Numérique et libertés : un nouvel âge démocratique*, rapport n° 3119, présenté par Christian Paul et Christiane Féral-Schuhl, spéc. pp. 131 et s.

[48] Article 54 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique :
« *L'article 1er de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est complété par un alinéa ainsi rédigé : « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi*. » ».

[49] Pauline Türk, "L'autodétermination informationnelle : un droit fondamental émergent ?", *Dalloz IP/IT*, n° 11, 1er novembre 2020 p.616-620) ? Avec plaisir et pardon pour l'oubli ! Je suis tout à fait favorable aux débats doctrinaux !

caractère davantage négatif, il joue un rôle uniquement de limite des données d'un individu qui peuvent être traitées ou non. En Allemagne, la « théorie des sphères »[50] (*Intimsphäre – Privatsphäre - Individualsphäre*), qui a précédé l'invention jurisprudentielle de l'autodétermination informationnelle, s'apparentait pendant longtemps à cette conception « mur » de la vie privée à la française[51]. Or, la Cour constitutionnelle fédérale allemande (BVerfGE) est allée bien plus loin, dans une décision de 1983, en constatant que le problème du traitement informatique des données personnelles est davantage une question de perte de maîtrise des informations que nos données fournissent aux tiers et à l'État qu'une question de révélation d'éléments de notre vie intime. La théorie des sphères a depuis lors été abandonnée comme outil interprétatif des atteintes portées aux droit fondamentaux par le traitement de données personnelles au profit de l'autodétermination informationnelle[52].

Précisément, la BVerfGE a affirmé que « la non-transparence sur la circulation des informations est contraire non seulement au droit au libre développement de la personnalité mais aussi à l'intérêt général, puisque l'autonomie de la personne est la condition fondamentale de toute société libre et démocratique qui est fondée sur la possibilité de ses membres d'y agir et d'y participer. Celui qui n'est pas en mesure de savoir si des comportements déviants sont enregistrés, évitera toute activité qui pourrait être considérée comme déviante » (cons. 155)[53].

Sans faire ici ni un historique ni un résumé de la jurisprudence constitutionnelle fédérale allemande, il convient seulement d'interroger ce droit au moyen de deux arguments :

- Tout d'abord, comment éviter le risque de réduire ce concept en un vœu de droit ? Autrement dit, comment le rendre effectif ? À l'heure où ces lignes sont écrites, l'autodétermination informationnelle pourrait être la consécration supra-législative d'une utopie. En effet, les composantes de l'autodétermination informationnelle dont nous disposons grâce au cadre légal (consentement, droit à l'information, droit à la portabilité, droit à l'effacement) sont davantage des fictions que des réalités concrètes. Nous savons que les centaines de consentements que nous faisons par jour ne sont pas « libres, spécifiques, éclairés et univoques » ; que le droit à l'effacement connaît des limites territoriales et de conciliation avec d'autres droits ; que le droit à l'information adressé au responsable de traitement peut prendre des mois, voire des années, avant d'être satisfait. Nous adhérons ainsi aux propos d'Orla Lynsley lorsqu'elle trouve fallacieux[54] de promouvoir l'idée de contrôle des données par les individus en raison des asymétries qui persistent entre ces derniers et les responsables de traitements ; des asymétries qui s'accentueront si on laisse aux individus le contrôle de leurs données. De même, nous rejoignons les propos de Jean-Philippe Foegle qui parle de « fonction rhétorique de légitimation » du droit à la protection des données personnelles par le biais du concept d'autodétermination

[50] Sur la théorie des sphères, voir à titre indicatif : Christoph Gusy, « La théorie des sphères », *Annuaire international de justice constitutionnelle*, « Lutte contre le terrorisme et protection des droits fondamentaux – La protection de la vie privée », 2003, pp. 467-484 ; Constance Grewe, « Rapport-Allemagne », *Annuaire International de justice constitutionnelle*, « Constitution et secret de la vie privée », 2001, pp. 135-152 ; Hans Hubmann, *Das Persönlichkeitsrecht*, 2. Aufl., Böhlau Verlag, 1967, pp. 269 et s. ; Max-Emanuel Geis, « Der Kernbereich des Persönlichketsrechts », *JZ*, 1991, pp. 112 et s. ; Spiros Simitis, *op. cit.*, p. 271.

[51] Même si à cette époque en France le droit au respect de la vie privée n'avait pas encore trouvé un rattachement constitutionnel stable.

[52] Pour l'historique de ce processus d'invention jurisprudentielle, voir Christina Koumpli, thèse, *op. cit.*, pp. 100-108.

[53] BVerfGE 65,1, *Volkszählungsurteil*.

[54] Orla Lynskey, *The foundations of European Data Protection Law*, Oxford University Press, coll. « Oxford Studies in European Law », 2015, 336 p.

informationnelle[55]. La critique de ce concept n'est donc pas absente du débat, même dans son pays d'origine. En effet, Hans Peter Bull, premier Commissaire fédéral à la protection des données, a publié un ouvrage intitulé *Autodétermination informationnelle : vision ou illusion* ?[56].

- S'agissant du second argument qui peut être avancé pour nuancer ce droit « séducteur », il convient de noter qu'au regard de ces asymétries entre personnes concernées et responsables des traitements, consacrer l'autodétermination informationnelle reviendrait à abandonner l'individu dans la « jungle du tout numérique » ; ceci d'autant plus que les compétences préventives des autorités représentatives de l'intérêt général (telles que les autorités administratives indépendantes) sont désormais remplacées par la logique d'*accountability* consacrée par le RGPD, un élément du nouveau « droit de la compliance ».

c) Une tradition constitutionnelle commune ?

Une chose est cependant certaine à l'issue de cette comparaison de concepts : la « préoccupation anthropocentrée » - que ce soit à travers la vie privée, la privacy, ou l'autodétermination informationnelle - est un dénominateur commun au rattachement supra-législatif de la protection des données à caractère personnel au sein des trois ordres juridiques nationaux considérés, à l'opposé de la « génétique conciliatrice » de cette protection au sein de l'Union (qui revêt, comme on l'a vu, une double fonction de réalisation simultanée d'objectifs antinomiques).

Cette préoccupation pourrait ainsi former une tradition constitutionnelle commune aux États membres en vertu de l'article 6§2 du TUE[57] et ainsi constituer un apport intéressant à l'appréciation du niveau de protection des données personnelles accordé, sachant que l'UE privilégie la libre circulation au détriment des libertés des citoyens européens[58].

III. L'AMBIGUÏTE COMME OCCASION : ATTRIBUER UNE FONCTION COLLECTIVE A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Ayant mis en question à la fois la vie privée, la *privacy* et l'autodétermination informationnelle en tant qu'éléments pertinents en vue de trouver le sens de ce droit fondamental « nouveau », nous avons néanmoins relevé et retenu un dénominateur commun à ces concepts : le caractère

[55] Jean-Philippe Foegle, « Le "droit" à l'autodétermination informationnelle et les réseaux numériques », *in* Rafael Encinas de Munagorri, Alexandra Bensamoun, Estelle Brosset, Marie-Anne Cohendet, *Sciences et droits de l'homme*, Ed. Mare & Martin, 2017, p. 85-103, spéc. pp. 94 et s.

[56] Hans Peter Bull, *Informationelle Selbstbestimmung – Vision oder Illusion ?, Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit*, 2.aktualisierte Auflage; 2011. IX, Mohr Siebeck 142 s.

[57] « *L'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales et tels qu'ils résultent des traditions constitutionnelles communes aux États membres, font partie du droit de l'Union en tant que principes généraux* ».

[58] Les deux jurisprudences *Schrems* sont particulièrement illustratives de ce risque, qu'on laisse persister jusqu'à l'intervention de la CJUE. Tel est également l'exemple récent des décisions d'adéquation du Royaume-Uni au RGPD et à la Directive « Police Justice » qui mériteraient, de notre point de vue, une invalidation par la CJUE. En ce sens, voir Christina Koumpli, « L'impact du Brexit sur la protection des données à caractère personnel. Entre Scylla et Charybde », *in* Vanessa Barbé et Christina Koumpli, *Le Brexit et les droits et libertés*, Bruxelles, Bruylant, coll. « Colloques – Droit de l'Union européenne » (parution printemps 2022).

anthropocentré (*ἄνθρωπος* – ánthrōpos = l'être humain) de la protection des données à caractère personnel dans les traditions juridiques étatiques.

Or, il convient d'insister sur la dimension collective du risque qu'implique le traitement de ce type de données pour l'Homme et le citoyen de la société contemporaine ; une dimension qui manque dans la plupart des ordres juridiques actuellement, à l'exception de celui de l'Allemagne puisque en 1983, dans sa décision précitée, la BVerfG avait déjà souligné le risque au regard de la démocratie du traitement des données à caractère personnel.

On pourrait ainsi *in fine* profiter de cette ambigüité qui existe encore sur ***ce*** qui est protégé par l'article 8 de la CDFUE pour lui donner une réelle utilité face aux évolutions des technologies numériques qui, soyons réalistes, ne se préoccupent plus du rapport d'identification direct ou indirect entre une donnée et une personne physique (le RGPD est presque un texte déjà obsolète au regard des usages actuels des données des individus)[59].

En effet, aujourd'hui l'industrie de l'intelligence artificielle (IA) a résolu le casse-tête des limites de l'anonymisation des données personnelles (et donc du risque de non-conformité au RGPD) grâce au concept de « *synthetic data* »[60] selon lequel les données préservent les propriétés et l'utilité statistique de l'ensemble des données personnelles originelles (servant à la création du « *data set* » de données synthétiques), tout en faisant parfaitement face à la problématique de la *privacy* puisqu'il s'agit de données *a-personnelles* générées à partir de vraies données personnelles (en ce sens *synthétiques)* mais dont le lien identifiant n'existe pas et n'intéresse plus[61].

Ces technologies ne portent pas une atteinte individuelle à la vie privée des personnes (dont les données ont servi à la création de *datasets*), puisque le rapport est coupé entre personne et données. Or, elles pourraient porter une atteinte collective à l'Homme (et non plus à l'Individu) dans la mesure où elles contribuent à la création d'algorithmes discriminants. En effet, cette atteinte résulterait du fait que les « données synthétiques » peuvent produire des différenciations, certes rentables mais restreignant potentiellement la liberté des individus cibles (qui sont différents de ceux dont proviennent initialement les données) ; ces différentiations peuvent se mesurer à la fois en termes de libre accès à l'information (qui est l'une des conditions de la participation à la vie démocratique), en termes d'égal accès au travail, en termes d'égal accès à la propriété, en termes d'égal accès aux assurances et bientôt aux soins.

On sera donc d'accord avec les affirmations de Martin Tisné selon lesquelles les *data* constituent « le nouveau CO_2 ». Ce parallèle est très pertinent, l'auteur soulignant que « comme les émissions de dioxyde de carbone des industries d'un pays voisin peuvent être plus néfastes que notre empreinte carbone individuel, notre propre consentement au traitement des données n'est pas aussi néfaste que les milliers de consentements d'autres personnes ». La stratégie européenne visant à renforcer nos droits individuels (par le biais du RGPD) ne parvient pas à protéger des risques sociétaux générés par l'usage de nos données. L'auteur préconise ainsi des

[59] Axel Voss, *op. cit.*

[60] Source : https://www.accenture.com/us-en/blogs/technology-innovation/driving-real-value-with-synthetic-data ; https://www.accenture.com/_acnmedia/PDF-148/Accenture-Insilico-Faster-And-Cheaper.pdf ; https://arxiv.org/pdf/2011.07018.pdf ; Fernando Lucini, « The real deal about synthetic data », *MIT Sloan Management Review*, Winter 2022, pp. 6-8

[61] Nazmiye Ceren Abay, Yan Zhou, Murat Kantarcioglu, Bhavani Thuraisingham, and Latanya Sweeney, « Privacy preserving synthetic data release using deep learning », *in* Joint European Conference on Machine Learning and Knowledge Discovery in Databases. 2018, Springer, pp. 510-526

législations tenant compte des enjeux sociétaux et non plus individuels, en prenant le droit de l'environnement qui impose une logique de réduction mondiale d'émissions de CO_2[62] comme modèle à suivre.

La problématique ici n'est donc pas celle de la vie privée, de la *privacy* ou de l'autodétermination informationnelle ; cela n'apporte rien si l'on n'intervient pas de façon verticale afin d'imposer un cadre juridique (et non pas uniquement éthique) à la « dépersonnalisation des données à caractère personnel », c'est-à-dire aux usages permis et interdits de la dépersonnalisation des données, de cette capacité de rupture que les technologies numériques permettent entre la personne et ses données.

Le concept de « risque de dépersonnalisation des données » pourrait ainsi jouer un rôle de « noyau essentiel » du droit fondamental à la protection des données à caractère personnel (qu'il convient d'approcher indépendamment de la rentabilité des données). Il est le produit d'une longue observation historique et comparative des catégorisations réalisées par les législateurs sur des données et des traitements bénéficiant d'une protection accentuée : les données sensibles[63]. En effet, le constat que les législateurs ont soumis certaines données à un régime de garantie renforcée permet de percevoir qu'en effet, la problématique de la vie privée n'est que secondaire.

Or, ce risque de « dépersonnalisation des données à caractère personnel » est difficilement quantifiable, difficilement défendable en justice et réparable, d'où certainement le fait qu'il reste sous silence. Il est néanmoins présent malgré son invisibilité et il était même perçu par les premiers législateurs nationaux, notamment le législateur français lorsqu'il prévoyait, on l'a vu, que « *l'informatique doit être au service de chaque citoyen* » (loi informatique et libertés, version originale). N'est-il donc pas temps de cibler les cas dans lesquels l'informatique ne serait pas au service du citoyen ?

Il est certain que les enjeux sociétaux du numérique interrogent la complétude de l'arsenal juridique en termes de droits fondamentaux. La consécration d'une déclaration des droits et principes numériques par les institutions européennes en janvier 2023 démontre l'actualité de la question posée par ce colloque ayant eu lieu plusieurs mois auparavant.

Or, à notre sens, les droits fondamentaux existants peuvent suffire pour poser les limites nécessaires aux dangers du numérique, à condition que leurs interprètes se tâchent à en définir le sens du seul point de vue de l'humain.

L'exemple du droit à la protection des données à caractère personnel, dont il a été question ici, a permis de constater qu'il est plus urgent de dessiner ses contours et de le « purifier » d'amalgames hétérogènes introduits par le droit de l'UE avant de chercher à le mettre à jour par la consécration d'autres droits.

Surtout il est essentiel de prendre conscience que le traitement des données personnelles peut porter atteinte à une multitude de droits fondamentaux traditionnels, autres que le droit au respect de la vie privée ; il serait ainsi temps que les juges les repèrent et les nomment

[62] Martin Tisné, « The Data Delusion: Protecting Individual Data Isn't Enough When The Harm is Collective », publication en ligne du Cyber Policy Center, Standford University, 12 p., disponible sur: https://cyber.fsi.stanford.edu/publication/data-delusion [consulté le 27/2/22].

[63] Ce concept fait partie des propositions centrales de l'auteure, voir Christina Koumpli, thèse, *op.cit.*, pp. 247 et s.

expressément lors d’équilibre des intérêts que leurs décisions consacrent, sans s'en embusquer derrière la modernité du « droit à la protection des données personnelles » dont le sens reste équivoque.