50 ans de législations européennes de protection des données

Poullet, Yves

Published in:
Numérique, droit et société

Publication date:
2022

Document Version
le PDF de l'éditeur

50 ans de législations européennes de protection des données

Hier, aujourd'hui et demain

YVES POULLET

Professeur émérite à l'Université de Namur, professeur associé à l'UC Lille, coprésident du Namur Digital Institute, membre de l'Académie royale de Belgique

1. Oser en quelque quarante pages retracer 50 ans de vie d'un concept si riche mais également tellement relatif aux données d'évolution tant de la société que de la technologie est un défi. Nous entendions le relever en nous interrogeant également sur son devenir à l'heure où l'irruption souhaitée mais pleine de risques de l'intelligence artificielle bouleverse l'économie de législations à peine rédigées. Notre propos n'entend pas relater l'ensemble des événements qui ont marqué l'histoire législative et jurisprudentielle de la protection des données ni même, à propos des événements et thèmes retenus, procéder à une recension complète des écrits et documents à ce propos. Il nous suffit d'indiquer ce qui nous apparaît être les tendances majeures et à leurs propos, opérer une lecture très sélective des sources.

L'histoire de nos législations européennes[1] balaie diverses époques et quelques documents majeurs la jalonnent.

L'article 8 de la Convention européenne des droits de l'homme (Conv. EDH 1950) consacre la vie privée. Il nous importera d'en préciser l'approche centrée sur la création d'un espace privé individuel inviolable.

C'est à partir de ce concept que se conçoivent les premières législations de protection des données. On cite sans être exhaustif la loi du land de Hesse (1970), celles suédoise (1973), et française : loi dite « Informatique et

1. Nous n'aborderons pas ici les législations particulières relatives aux traitements effectués par la police ou la justice pénale ni celles relatives aux services d'intelligence ou de renseignement militaire.

libertés » (1978). À ces législations nationales, tant les principes directeurs de l'OCDE (1980) que la convention n° 108 du Conseil de l'Europe (1981), que deux résolutions, l'une relative au secteur public, l'autre au secteur privé dès 1973 et 1974 avaient précédés, devaient donner une légitimité internationale et ouvrir aux besoins d'une approche internationale.

Un troisième temps s'ouvre avec la volonté de l'Union européenne de construire un « modèle » de protection des données plus en lien avec les besoins de protection nés des avancées technologiques, ainsi la directive 95/46 de 1995 et la directive e-Privacy de 2002. Cette volonté aboutit à la consécration quasi constitutionnelle de la notion, comme droit distinct de celui de la vie privée. La Charte en effet proclame la protection des données à caractère personnel comme un droit quasi constitutionnel à part entière distinct de celui de la vie privée. Ainsi, à l'article 7 de la Charte des droits fondamentaux de l'Union européenne, adoptée le 12 décembre 2007[2] qui reprend le texte de l'article 8 de la Convention européenne des droits de l'homme, a été ajouté un article 8 qui consacre le droit à la protection des données de manière distincte[3] :

> « 1. Toute personne a droit à la protection des données à caractère personnel la concernant ;
>
> 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données la concernant et d'en obtenir la rectification ;
>
> 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

La distinction est encore renforcée par la consécration à l'article 16 du traité de Lisbonne[4] d'un droit « autonome » à la protection des données :

> « 1. Toute personne a droit à la protection des données à caractère personnel la concernant. Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement de données à caractère personnel par les institutions, organes et organismes de l'Union ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application de l'Union et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes. »

2. *JO* C-302, 14 déc. 2007. On sait que la Charte est jugée comme ayant une valeur « quasi constitutionnelle ».

3. Cette consécration a été fortement souhaitée par le Groupe dit de l'article 29 qui rassemble des représentants des différentes autorités indépendantes des États membres de l'Union européenne. Comme l'affirme la recommandation 4/99 du 7 sept. 1999 de ce Groupe : « *Inclusion of data protection among the fundamental rights of Europe would make such protection a legal requirement throughout the Union and reflect its increasing importance in the information society.* » La consécration d'un droit autonome s'explique aussi par le rejet d'une proposition allemande qui souhaitait refonder l'article sur la vie privée en droit à l'autodétermination.

4. *JO* C-115, 9 mai 2009. Cet article a été inséré dans le traité de la Communauté européenne en remplacement de l'article 286.

Sans doute, l'adaptation aux besoins de protection de notre vie privée et de nos données s'est-elle révélée rapidement insuffisante ou plutôt dépassée par les progrès technologiques. Sans doute, les disparités d'application de la directive avaient conduit la Commission à conclure à la nécessité d'un instrument ayant un effet direct sur l'ensemble du territoire de l'Union européenne[5]. Dès 2012, les acteurs institutionnels européens se remettaient à l'ouvrage pour aboutir en 2016 à l'adoption du Règlement général de protection des données (le RGPD), en vigueur depuis juin 2018. Le mouvement s'arrête-t-il là ? Cinq ans après l'adoption du RGPD, des préoccupations nouvelles voient le jour. La confrontation des dispositions du RGPD face en particulier aux enjeux liés à la multiplication des applications de l'IA introduit une mise en question du « modèle européen » ou plutôt son infléchissement.

2. Face aux transformations sociétales qu'induisent les progrès technologiques et que le droit doit, certes sans se hâter, prendre en compte, nous tentons de répondre à deux questions. Jetant un regard vers le passé, nous chercherons à montrer comment, à travers tous les textes cités, les concepts et les principes de nos législations de protection des données ont évolué. Dans le même temps, nous tournant vers le futur, nous nous interrogerons sur le bien-fondé mais également les lacunes du « modèle » européen. Dans une société du « tout numérique », de l'internet des objets, des NBIC, de l'intelligence artificielle, de la *blockchain*, au temps d'applications comme la reconnaissance faciale, la voiture intelligente, le profilage dans tous les domaines, les *hypernudges*, la manipulation génétique, comment aborder ce qui nous apparaît l'objectif même du droit à la vie privée et par là de nos législations de protection des données, à savoir offrir à chacun, individuellement mais surtout collectivement, une maîtrise de son environnement informationnel et au-delà une capacité de développement personnel grâce aux outils que l'innovation technologique nous présente pour le meilleur et pour le pire ?

3. Pour répondre à ces deux interrogations, le développement suivant est proposé, sans grande originalité. Le premier chapitre étudie brièvement l'évolution des rapports entre les désormais deux droits fondamentaux : celui de la vie privée et celui de la protection des données. Ensuite, nous examinerons les divers éléments qui sous-tendent le droit à la protection des données : la notion de données dite « à caractère personnel » et les acteurs pris en compte

5. L'affirmation n'est pas neuve. V., dès 2003, les remarques de la Commission européenne (Commission of the European Communities, First report on the implementation of the Data Protection Directive [95/46/EC], COM[2003] 265 final, Brussels, 15 may 2003).

par ces législations (II). Le troisième chapitre étudie la façon dont ont évolué, d'une part, les principes et obligations encadrant le droit au traitement des responsables de traitement et, d'autre part, ce que dans un récent article, M^me^ Eynard[6] appelait l'« empouvoirement » des personnes concernées. Il nous restera (IV) à dire quelques mots sur les instruments d'effectivité de nos législations, en particulier deux points : le rôle croissant des autorités de protection des données et la dimension dite « extraterritoriale » d'un modèle européen, de plus en plus « impérialiste ».

I. VIE PRIVÉE *VS* PROTECTION DES DONNÉES : DEUX DROITS FONDAMENTAUX OU LA PROTECTION DES DONNÉES, DROIT DÉRIVÉ ?

4. En consacrant la vie privée comme un droit fondamental[7], la Convention européenne du Conseil de l'Europe entendait répondre à l'attente d'une société libérale qui, au sortir de la Seconde Guerre mondiale et des exactions y commises, réclamait la possibilité d'un espace clos indispensable au développement de nos personnalités et inviolable par l'État. L'espace privé se distinguait, dans l'esprit des auteurs, de celui public. « La distinction entre le public et le privé, écrit B. Rey[8], émerge à l'Époque moderne. La tradition politique libérale s'est basée sur la distinction nette entre ces deux sphères, apparue au sein de la bourgeoisie urbaine des grandes villes européennes des XVI^e^ et XVII^e^ siècles. La notion de vie privée a été culturellement et historiquement construite comme une valeur sociale appréciée et recherchée et a été inscrite au rang des droits humains fondamentaux, dans un mouvement complexe centré sur un domaine privé incarné d'abord par la famille, puis par l'espace individuel. »

5. Ainsi, le concept de vie privée se définit à l'origine de manière restrictive et négative : il s'agit de défendre l'intimité de la personne, *« the right to be let alone »*, en protégeant ainsi, certains lieux, la maison qui protège outre

6. J. Eynard, « "Empouvoirement" individuel », dossier spécial sous la direction de C. Castets, *Rev. aff. eur.* 2021, n° 1, p. 21 s.

7. Article 8.1. : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. »

8. B. Rey, *La vie privée à l'ère du numérique*, Paris, Lavoisier, 2012. Sur une analyse complète de l'évolution de la notion de vie privée, lire l'ouvrage en trois volumes édité sous la direction de P. Ariès et G. Duby, *Une histoire de la vie privée*, Seuil, 1986 (en anglais *A History of Private Life*, R. Chartier, Cambridge, The Bellknap Press of Harvard University Press, 1987), en particulier le volume III qui analyse les tendances contemporaines et celui de C. J. Bennett et C. Raab, *The Governance of Privacy. Policy Instruments in Global Perspective*, MIT Press, 2003. On citera sur l'histoire de concept de *privacy* en droit américain, l'article de D. J. Solove, « GW LAW Scholarly Commons », Washington, 2006.

la personne, les relations familiales qui s'y nouent ou se dénouent ; ainsi, la correspondance ou plutôt la communication entre personnes privées ; ainsi certaines données dites sensibles dans la mesure où elles concernent l'intimité de la personne. Le concept se conçoit de manière négative, soit comme le refus à autrui et en particulier à l'État, de pénétrer ces « lieux » ou d'utiliser ces « données ». Il s'agit d'édifier autour de chaque individu, un « jardin clos », physique et communicationnel, où chacun peut s'épanouir à l'abri du regard d'autrui. À l'inverse, le droit de la protection des données entend, de manière positive cette fois, affirmer dans le même mouvement, d'une part, l'existence du droit de traiter les données d'autrui certes sous nombre de conditions et entraînant des obligations nombreuses sur lesquelles nous reviendrons (*infra*, n^os^ 16 s.) mais surtout le droit de la personne concernée à la maîtrise de cet usage de ses données à travers la consécration de nombreux droits subjectifs (*infra*, n^os^ 20 s.). C'est là l'argument avancé par nombre d'auteurs pour distinguer le « vieux » droit à la vie privée de celui plus moderne qui, de manière réaliste, considère que nos sociétés devenues sociétés de l'information ne peuvent se contenter de dresser un jardin clos mais, au regard de la circulation légitime de données dont le sens ne cesse de se renouveler au gré de leur circulation sur la toile tissée par nos infrastructures de communication et de leurs agrégations avec d'autres données, réclament un droit de chacun à l'autodétermination informationnelle, comme l'a consacré le tribunal constitutionnel allemand, dès 1983[9].

6. Cette distinction de deux droits fondamentaux est consacrée par la Charte européenne des droits fondamentaux, comme nous l'avons dit. À cet égard, l'évolution, le passage d'une conception de la protection des données, dérivée de la protection de la vie privée vers une autonomisation des deux concepts, s'opère progressivement. Les premiers textes du Conseil de l'Europe reconnaissant le droit à la protection des données, soit les résolutions de 1973 et 1974[10] et la convention n° 108[11], se réfèrent à la nécessité de donner pleine effectivité au droit fondamental à la vie privée lorsqu'il s'agit de traitement

9. Il s'agit du fameux arrêt sur le recensement statistique, publié in *BVerfGE*, 65, I. Le texte anglais a été publié in *Human Rights Law Journal*, 1984, p. 94 s. (avec le commentaire de E. Riedel, « Census Act 1983 Partially Unconstitutional »). Pour un autre commentaire de la décision, S. Simitis, « Die informationelle Selbstbestimmung. Grundbedingungen einer verfassungskonformen Informationsordnung », *NJW* 1984, p. 398-405.

10. *« Bearing in mind Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, Recommends the governments of member states : a. to take all steps which they consider necessary to give effect to the principles set out in the annex to the present resolution »* (préambule de la résolution de 1974).

11. V. à cet égard, l'article 1 de la convention n° 108 qui n'a pas été modifié lors de la révision de cette convention en 2018 : « 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"). »

automatisé des données à caractère personnel la concernant. Dans l'esprit des auteurs des premiers textes, l'exigence de protection des données dérive de l'impératif de la vie privée. Cette corrélation disparaît progressivement. La directive de 1995 en son article 1 et le RGPD en son considérant n° 4[12] épinglent certes la vie privée mais parmi l'ensemble des droits et libertés fondamentaux. Le texte de la directive mentionne la vie privée à treize reprises ; celui du règlement, seulement quatre fois. Qu'est-ce à dire ? Faut-il définitivement consacrer la scission des deux droits et les placer sur un pied d'égalité ?

7. Nous ne le pensons pas[13]. Sans vouloir ici résumer le long argumentaire publié il y a deux ans[14], trois arguments nous paraissent devoir être retenus. *Premier argument* : nous pensons que la conception restrictive de la vie privée défendue par les partenaires de la distinction s'arrête à une interprétation étriquée du concept de vie privée, alors même que la jurisprudence de la Cour de Strasbourg a depuis longtemps développé une approche large, innovante et évolutive de la notion[15]. « Comme la Cour a déjà eu l'occasion de l'observer,

12. *JO* C-115, 9 mai 2009. Cet article a été inséré dans le traité de la Communauté européenne en remplacement de l'article 286.

13. En ce sens également, G. Gonzales Fuster et H. Hijmans, « The EU rights to privacy and personal data protection : 20 years in 10 questions », *Discussion paper, International Workshop 'Exploring the Privacy and Data Protection connection : International Workshop on the Legal Notions of Privacy and Data Protection in EU Law in a Rapidly Changing World' of 14th May 2019*, co-organised by the Brussels Privacy Hub (BPH) and the Law, Science, Technology and Society (LSTS) Research Group at the Vrije Universiteit Brussel (VUB) : « Actually, all human rights are connected, and the right to privacy and the right to personal data protection are particularly deeply interconnected, and in a way tend to converge. *The two rights are clearly coupled in the relevant case law of the CJEU, where they are not systematically distinguished – and where they are occasionally presented in complex interwoven manners.* »

14. Y. Poullet, *La vie privée à l'heure du numérique*, Essai, Collection du CRID, n° 45, Bruxelles, Larcier, 189 p. Cet ouvrage a obtenu le prix O. Debouzy de l'agitateur d'idées juridiques de l'année 2019.

15. Sur cette interprétation jurisprudentielle créative, lire l'ouvrage : *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, coll. « Droit et Justice », n° 63, Bruxelles, Bruylant-Nemesis, 2005, p. 72. L'analyse de la jurisprudence du Conseil de l'Europe en atteste. Pour reprendre le résumé du professeur Sudre qui introduit l'ouvrage cité (p. 27 s.), « l'examen de la jurisprudence européenne amène à constater un usage quasi systématique par le juge européen de la technique des obligations positives dont on sait qu'elle emporte une redéfinition des obligations des États parties. Les obligations positives se déploient quel que soit le domaine de la "vie privée"... Ainsi, sans aucune prétention d'exhaustivité, on cite l'obligation de rendre les lieux publics accessibles aux personnes handicapées (Affaire Zehnalova), celle de donner les informations aux candidats aux logements de la présence d'industries aux activités potentiellement nuisibles (Affaire Guerra), celle d'interdire à l'employeur la surveillance des conversations de ses employés (Affaire Copland), etc. Il s'agit bien à travers ces obligations de donner effectivité aux garanties qu'exige le développement de la personnalité et, le cas échéant, de créer dans le chef des individus des droits subjectifs nouveaux dont l'exercice garantira la protection de la vie privée ».

la notion de "vie privée" est une notion large, non susceptible d'une définition exhaustive. Elle recouvre l'intégrité physique de la personne [...]. Elle peut parfois englober des aspects de l'identité physique et sociale d'un individu [...]. Des éléments tels, par exemple, l'identification sexuelle, le nom, l'orientation sexuelle et la vie sexuelle relèvent de la sphère personnelle protégée par l'article 8 [...]. Cette disposition protège également le droit au développement personnel et le droit d'établir et d'entretenir des rapports avec d'autres êtres humains et le monde extérieur [...]. Bien qu'il n'ait été établi dans aucune affaire antérieure que l'article 8 de la Convention comporte un droit à l'autodétermination en tant que tel, la Cour considère que la notion d'autonomie personnelle reflète un principe important qui sous-tend l'interprétation des garanties de l'article 8. » Comme le note F. Sudre, « la notion d'autonomie personnelle semble érigée en principe matriciel du droit garanti par l'article 8 et l'on est alors tenté de penser que la jurisprudence européenne a franchi le pas, du droit d'être laissé seul au droit à l'autodétermination ». Or le droit à l'autodétermination décliné en droit à l'autodétermination informationnelle n'est-il pas la définition que certains souhaitent mettre en avant pour définir le droit à la protection des données. Les juges de la Cour de justice européenne[16] ne s'y trompent pas lorsqu'à l'occasion de litiges relatifs à la protection des données, ils maintiennent une référence tant à l'article 7 qu'à l'article 8 de la Charte.

8. Passer de la conception d'un droit à l'intimité à un droit au libre épanouissement qui englobe le droit à l'intimité semble résumer l'évolution de la jurisprudence de la Cour de Strasbourg. De là nous tirons un *deuxième argument*. Il nous apparaît en effet dangereux de séparer l'approche négative (protéger contre l'intrusion d'autrui) de l'approche plus positive (accepter mais baliser et contrôler les traitements de données), alors que ces deux approches sont liées et se légitiment par leur objectif commun de permettre à la personne de s'épanouir ou, selon l'expression de la Cour européenne des droits de l'homme dans l'affaire Barbulescu, le droit de l'individu « de

16. À ce propos, le relevé des décisions de la CJUE qui maintiennent cette double référence et l'appui à cette approche, C. de Terwangne, « Internet et la protection des données à caractère personnel », *in* C. de Terwangne et Q. van Inis (dir.), *L'Europe des droits de l'homme à l'heure d'internet*, p. 330 s. On note cependant un arrêt de 2015 : « les notions de données à caractère personnel [...] et de données relatives à la vie privée ne se confondent pas » (CJUE 16 juill. 2015, *ClientEarth*, aff. C-615/13 P, pt 32). On ajoute le même mouvement de double rattachement dans la jurisprudence de la Cour constitutionnelle française : « Si, en France, la jurisprudence du Conseil constitutionnel n'a pas détaché la protection des données personnelles de celle de la vie privée, en Europe, la Charte des droits fondamentaux de l'Union européenne sépare les deux notions : l'article 7 consacre le respect de la vie privée, quand l'article 8 élève la protection des données personnelles comme droit fondamental » (à propos de l'ouvrage de B. Rey et I. Ferhat, *La construction historique des notions de vie privée et de protection des données personnelles*, p. 11, disponible sur : [https://journals.openedition.org/lectures/10542]).

forger son identité sociale par le développement de relations avec autrui[17] ». Ainsi, pour revenir à la question des liens entre les concepts de vie privée et de protection des données à caractère personnel, le concept de vie privée entendu comme « droit à l'épanouissement de la personnalité » ou comme le qualifie la Cour, également dans l'affaire Pretty, de droit à la « qualité de la vie »[18], ne se limite pas à la vie privée – INTIMITÉ par opposition à la vie privée ou protection des données – CONTRÔLE. Il s'agit bien de montrer le lien essentiel entre ces deux facettes de la vie privée, chacune également importante pour garantir l'épanouissement de la personnalité[19]. Ce point est important tant on peut regretter que les débats autour de la protection des données oublient sans doute trop cette dimension intimiste de la vie privée pourtant bien nécessaire dans nos sociétés de surveillance ubiquitaire et continue de nos personnes, à savoir celle du droit à la déconnexion, celle du droit à l'oubli, celle de la protection garantie contre les intrusions dans nos terminaux[20].

9. Le *troisième et dernier argument* nous paraît plus essentiel encore. Énonçons-le ainsi : sans le raccrocher au droit fondamental à la vie privée, il appert que le droit à la protection des données perd son âme et apparaît

17. CEDH 7 sept. 2017, *Barbulescu c/ Roumanie*, req. n° 61496/08, § 71, dans une affaire relative à un contrôle par l'employeur de la correspondance électronique de son employé : « Des restrictions apportées à la vie professionnelle peuvent tomber sous le coup de l'article 8 lorsqu'elles se répercutent sur la façon dont *l'individu forge son identité sociale par le développement de relations avec autrui.* » Pour une justification de la nécessité de joindre les deux versants de la vie privée, à savoir celui d'être laissé seul et celui de pouvoir « maîtriser son environnement informationnel », lire A. Rouvroy et Y. Poullet, « The right to informational Self-determination and the value of Self-development : Reassessing the importance of Privacy for Democracy », in *Reinventing Data Protection ?*, Dordrecht, Springer, 2009, p. 159 s.

18. CEDH 2002, *Pretty*, n° 2346/02, III, § 61 : « La dignité et la liberté de l'homme sont l'essence même de la Convention... la Cour considère que c'est sous l'angle de l'article 8 que la notion de qualité de la vie prend toute sa signification. » ... « L'article 8 protège un droit au développement personnel et le droit à établir et à développer des relations avec d'autres êtres humains et avec le monde extérieur... Même si aucun précédent n'a établi comme tel un droit à l'autodétermination comme étant contenu dans l'article 8 de la Convention, la Cour considère que la notion d'autonomie personnelle est un principe important *à la base de l'interprétation des garanties offertes par cet article.* »

19. Comme le note J. Cohen (*Configuring the Networked Self, Law, Code and the Play of Everyday Practice*, New Haven CT, Yale University Press, 2012, p. 89), *« [i]n some contexts, human flourishing demands reduced openness ; in particular, human flourishing requires a reversal of the dynamic of one-way transparency, a rethinking of the principle of exposure, and a critical, revisionist stance toward the normative underpinnings of the culture of exposure. Human flourishing requires both boundedness and some ability to manage boundedness. Respect for privacy does not require absolute secrecy for personal matters. Rather, it entails something easier to imagine but more difficult to achieve : more openness about some things and less openness about others ».*

20. À cet égard, la décision du tribunal constitutionnel allemand du 27 févr. 2008, *BVerfGE*, 1 BvR 370/07, *RTDI* 2009. 88 s., note P. de Hert, K. De Vries et S. Gutwirth.

comme une revendication individualiste qui s'épuise dans l'énumération de droits opposés, ceux de la personne concernée, ceux des responsables de traitements, sans que la clé de leur équilibre ne soit énoncée à l'aune de l'objectif poursuivi. Ainsi, face aux technologies de la reconnaissance faciale, comment fixer les limites du droit des autorités publiques et privées à les utiliser ? Ne doit-on pas considérer cet arbitrage au regard de la dimension plus large à laquelle nous amène le concept élargi de vie privée, condition de développement de nos personnalités dans une société évolutive. Les législations de protection des données trouvent donc, dans le concept de vie privée entendue comme « exigence et garantie d'épanouissement personnel », leur fondement, la nécessité de leur interprétation et également la pertinence de leur évolution continue.

Le droit quasi constitutionnel à la protection des données n'est qu'un droit dérivé[21] de cette exigence première adressée à nos « États de droit » de protéger bien plus que les données, les personnes et d'envisager la vie privée comme une condition de survie de nos démocraties forte d'hommes libres. Si la vie privée protège l'individu, sa revendication n'est donc pas celle d'un droit purement individuel. Ce que la vie privée entend défendre c'est la construction d'une personnalité, agissante dans la vie sociale sans contraintes excessives conscientes ou inconscientes. Il s'agit là d'un combat dont l'ultime sens est collectif, permettre à chacun de participer, dans l'espace de liberté qui doit être le sien, à la construction de la démocratie[22]. L'enjeu essentiel du droit à la protection de la vie privée est la défense de l'humain, de son développement et de sa dignité comme valeurs absolues et le renvoi des logiques absolues de sécurité et d'efficacité économique à leur dimension toute relative.

21. Sur cette notion de « droit fondamental dérivé » ou plutôt « droits-gigognes », vu le danger de cette prolifération des droits consacrés comme droits fondamentaux et la perte induite de leurs valeurs, lire S. Turgis, « Les droits de l'homme à l'heure d'internet et du numérique : rupture ou continuité », *in* C. de Terwangne et Q. van Inis (dir.), *L'Europe des droits de l'homme à l'heure d'internet*, *op. cit.*, p. 93 s., en particulier, p. 116, l'application à la vie privée : « Sur le fondement d'un droit fondamental sont identifiées plusieurs composantes qui peuvent elles-mêmes englober d'autres éléments. La déclinaison pourrait sembler infinie. »

22. En ce sens, J. Habermas (*Between Facts and Norms*, MIT Press, 1996) parle de *« co-originality »* de l'autonomie publique et privée : *« And once this point is established, privacy's dynamism becomes clear. Lack of privacy means reduced scope for self-making – along the lines of the liberal ideal, or along other lines. Privacy does not negate social shaping. "In a world with effective boundary management, however, there is play in the joints, and that is better than the alternative... Privacy's goal, simply put, is to ensure that the development of subjectivity and the development of communal values do not proceed in lockstep." Privacy will not always produce expressions of subjectivity that have social value, and here I mean expressly to leave open the question whether there might be particular types of privacy claims that do not merit protection or even respect. Even so, privacy is one of the resources that situated subjects require to flourish »* (J. Cohen, « What Privacy is For ? », *Harvard Law Journal* 2013, n° 126, p. 1930. Dans le même sens, P. Schwartz, « Privacy and democracy in Cyberspace », *Vanderbilt Law Review* 1999, p. 52.

Le concept de « protection des données » centre le débat sur la donnée au risque de la consacrer comme un bien immatériel dont la personne concernée, chaque individu, serait propriétaire. Nous reviendrons sur cette approche individualiste du droit à la protection des données lors de notre analyse des droits subjectifs accordés par le RGPD aux personnes concernées.

II. DE LA DÉFINITION DE LA NOTION DE DONNÉE À CARACTÈRE PERSONNEL ET DES ACTEURS

A. LA NOTION DE DONNÉES À CARACTÈRE PERSONNEL

10. Cette notion a connu des modifications dans sa compréhension, qui sont loin d'être sans signification. Elles témoignent de la puissance croissante du numérique dans la dimension omniprésente de la collecte de données, y compris triviales, et dans sa capacité à en déduire des informations relatives à des individus indépendamment de leur identité. Avant d'aborder ces variations de compréhension et donc d'extension de la notion, un mot sur la restriction de la protection à un type de personnes, à savoir les personnes physiques, à l'exclusion des personnes morales. La question renvoie à une thèse défendue dès 1979[23] et esquissée à la suite de la lecture des législations dites de première génération, les législations luxembourgeoise, norvégienne et autrichienne et depuis italienne, qui admettaient la protection des personnes morales, protection que la directive *« e-Privacy »* reprend à son compte[24] mais dont on ne trouve pas de trace dans le RGPD consacré à la protection des seules données des personnes physiques. Or l'asymétrie de plus en plus grande entre le pouvoir informationnel de certaines entreprises qui ont le droit de vie et de mort sur d'autres entreprises, et, précisément, ces dernières, justifient, au nom de la protection de la liberté d'entreprendre mais également de la protection des employés de ces petites structures, que celles-ci puissent bénéficier de certaines prérogatives que le Règlement réserve pour le moment aux seules personnes physiques.

Certes, invoquer la « vie privée » des personnes morales paraît délicat et *« ultra legem »*, comme le rappelle un arrêt du 17 mars 2016[25] de la Cour

23. P. et Y. Poullet, « Applicabilité de la loi vie privée aux entreprises », in *Banque de données, entreprises et vie privée*, Bruxelles, CIEAU, 1979, p. 120 s.

24. La proposition de règlement e-Privacy devant modifier la directive e-Privacy reprend cette même extension. Sur cette extension et son interprétation, lire K. Rosier, « La notion de "données à caractère personnel" a-t-elle encore un sens ? », *in* E. Degrave, C. de Terwangne, S. Dusollier et R. Queck (dir.), *Droit, normes et gouvernance dans le cybermonde. Liber Amicorum Y. Poullet*, Cahiers du CRID, n° 43, p. 705.

25. A. Le Ninivin et A. Carteret, « Absence de protection générale de la vie privée des personnes morales », article rédigé le 29 juin 2016 et disponible sur : [https://larevue.squirepattonboggs.com/Absence-de-protection-generale-de-la-vie-privee-des-personnes-

de cassation française, qui avait à se prononcer pour la première fois sur la possibilité d'accorder le bénéfice de la protection de la vie privée, telle que prévue à l'article 9 du Code civil français, aux personnes morales[26]. Il est vrai que certaines décisions de la Cour de Strasbourg ont reconnu aux personnes morales, sur base de l'article 8 Conv. EDH, certaines protections, en particulier de la correspondance et du domicile[27][28]. Au regard des risques qu'entraîne l'asymétrie informationnelle, ne peut-on justifier une obligation positive de l'Union européenne ou des États de protéger les associations à but non lucratif et les entreprises, en particulier les petites et moyennes, des usages que pourraient faire de leurs données, certains « responsables de traitement » ? Il ne peut être question de copier l'ensemble des dispositions existantes en matière de personnes physiques mais sans doute d'octroyer aux personnes morales « concernées » certaines prérogatives similaires à celles de la personne physique (ainsi, les droits d'accès, de correction, le droit à l'oubli, etc.)[29].

morales_a2921.html] : « La propriétaire d'un immeuble attenant à une boulangerie avait fait installer une caméra qui surveillait l'entrée de l'immeuble. Or, la caméra captait également la porte arrière du fournil de la boulangerie. Cette dernière a donc saisi le juge des référés d'une demande tendant à faire reconnaître l'atteinte à sa vie privée, obtenir la cessation du trouble par le retrait de la caméra, et l'octroi d'une provision sur l'indemnisation du préjudice subi. Les demandes avaient été accueillies en appel, la Cour constatant une atteinte à la vie privée de la société, au visa de l'article 9 [1] du Code civil. »

26. La Cour de cassation précise que « si les personnes morales disposent, notamment, d'un droit à la protection de leur nom, de leur domicile, de leurs correspondances et de leur réputation, seules les personnes physiques peuvent se prévaloir d'une atteinte à la vie privée au sens de l'article 9 du code civil ».

27. À propos du domicile, voir l'affaire *Sté Colas c/ France* (16 avr. 2002). Se fondant sur l'article 8 de la Convention européenne de sauvegarde des droits de l'homme, portant sur la protection « de la vie privée et familiale, du domicile et de la correspondance », la Cour conclut que les personnes morales bénéficient de la même protection contre les ingérences dans leur domicile que les personnes physiques. En matière de correspondance, la CEDH reconnaît, dans un arrêt du 28 juin 2007, qu'une association, ayant la personnalité morale, pouvait bénéficier également de la protection de l'article 8 portant sur le secret des correspondances.

28. Ne peut-on fonder la protection des données relatives des personnes morales sur l'article 10 de la Charte européenne des droits de l'homme qui reconnaît la liberté d'entreprise ? On note que la convention du Conseil de l'Europe ne reconnaît pas explicitement cette liberté.

29. Sur ce point, v. les commentaires (n^{os} 31 s.) des lignes directrices de l'OCDE de 1980. Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel : « De l'avis de certains pays, la protection à accorder aux données relatives aux personnes physiques peut être de même nature que celle requise pour les données concernant les entreprises industrielles et commerciales, les associations et groupes qui peuvent ou non être dotés de la personnalité juridique. L'expérience acquise par un certain nombre de pays montre aussi qu'il est difficile de tracer clairement la ligne de démarcation entre les données de caractère personnel et celles qui ne le sont pas. Les données relatives à une petite entreprise, par exemple, peuvent également concerner son (ou ses) propriétaire(s) et fournir des informations de caractère personnel plus ou moins sensibles. Dans de tels cas, il pourra être souhaitable d'étendre aux organismes constitués en sociétés la protection offerte par des règles qui se rapportent principalement aux

11. Les premiers textes du Conseil de l'Europe, à savoir les recommandations de 1973 et 1974, et les premières législations entendent bien couvrir des données au-delà de ce qui à l'époque était compris comme les données intimes de la vie privée, les données qualifiées de données sensibles et dont la nature justifie le principe d'une interdiction de traitement. Cette distinction au sein des données à caractère personnel persiste. On notera cependant que la notion de données sensibles s'étend dorénavant avec le RGPD aux données biométriques et génétiques, au regard des risques majeurs liés aux traitements modernes de telles données, qu'on songe à la reconnaissance faciale[30] ou aux prédictions de santé qu'autorise désormais l'analyse de nos génomes.

Par ailleurs, la définition du RGPD semble marquer une évolution majeure d'une définition de la donnée sensible. Il s'agit d'abandonner une définition de la sensibilité de la donnée en fonction de sa nature au bénéfice d'une approche « finaliste ». Alors que la directive semblait se référer à une définition des données par leur nature, le RGPD adopte un autre point de vue lorsqu'il dispose que *« Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale... »*. C'est donc au sein du traitement et

données de caractère personnel. De même, on peut s'interroger sur la mesure dans laquelle les personnes appartenant à un groupe particulier (handicapés mentaux, immigrants, minorités ethniques, par exemple) doivent bénéficier d'une protection supplémentaire contre la diffusion d'informations concernant ledit groupe. En revanche, les lignes directrices reflètent le point de vue selon lequel les notions d'intégrité individuelle et de vie privée sont à maints égards particulières et ne devraient pas être traitées de la même manière que l'intégrité d'un groupe de personnes ou la sécurité des sociétés et le caractère confidentiel de leurs activités. Les besoins de protection sont différents, de même que le cadre dans lequel les solutions doivent être formulées et les intérêts doivent être conciliés [...]. »

30. Sur la nécessité d'une protection des données face aux développements des techniques de reconnaissance faciale, lire notamment l'avis de l'APD belge, disponible sur : [https://www.autoriteprotectiondonnees.be/professionnel/themes/le-droit-a-l-image/reconnaissance-faciale-et-droit-a-limage] : « Grâce aux techniques de reconnaissance faciale, nos visages sont transformés en données qu'il devient dès lors possible de regrouper, de classer et d'analyser. Si l'utilisation de la reconnaissance faciale peut s'avérer positive dans certains cas (lutte contre le terrorisme ou la fraude par exemple), il n'en reste pas moins qu'elle présente des risques pour le respect de notre vie privée. Ainsi, que penser d'entreprises privées qui détiennent à ce jour les plus grandes bases de données d'images ? Et de technologies de reconnaissance faciale qui permettent, à partir d'un nom, de retrouver sur le réseau et le web toutes les images représentants la personne ? Que penser également de l'utilisation de ces méthodes dans des lieux publics ? Il n'existe encore que peu d'opinion institutionnelle sur ces questions. Face à ces enjeux de protection des données et de risques d'atteintes aux libertés individuelles (comme la liberté d'aller et de venir), se posent aussi ceux de la sécurité de nos données en ligne et du risque de leur piratage ou de leur utilisation frauduleuse. C'est en raison du risque élevé lié au traitement de ces données que le RGPD a introduit l'obligation de recourir à une analyse d'impact relative à la protection des données (AIPD). » Nous reviendrons sur ces techniques fondées sur l'IA et leur réglementation par la proposition européenne dite *« Artificial Intelligence Act. »*

au vu de sa finalité que la donnée devient sensible[31]. À cette modification des critères de la sensibilité et à cette extension des données visées, correspond dans le sens inverse une diminution de leur protection par la multiplication des exceptions au principe d'interdiction. Le RGPD en mentionne dix, alors que la directive n'en retenait que 5, là où la convention n° 108 de 1981 (article 6) affirmait avec force le principe d'interdiction et s'en remettait au droit interne en exigeant de ce dernier qu'il offre des garanties appropriées.

12. Venons-en à la notion de données hier nominatives aujourd'hui à caractère personnel[32]. Les tout premiers textes restreignaient la protection aux données « nominatives ». Il s'agissait donc de limiter la protection à des données mentionnant l'élément essentiel de l'identité civile de la personne physique. Les résolutions de 73 et 74 du Conseil de l'Europe parlaient d'« informations personnelles », c'est-à-dire d'informations concernant un individu identifié.

La Convention élargissait déjà son champ d'application. La « donnée personnelle » est (article 2 a) « toute information concernant un individu identifié ou identifiable à condition qu'il s'agisse de moyens faciles et non de l'utilisation de moyens sophistiqués[33] ». Ainsi, ce qui était important n'était plus le fait que la donnée en elle-même contienne une référence à l'identité civile de la personne ou à un élément de celle-ci mais qu'elle permette aisément de retrouver cette identité civile, ainsi le numéro d'identification d'un client.

La directive devait encore élargir le concept. Tout d'abord, elle adopte l'appellation de « donnée à caractère personnel ». Ce n'est plus par leur contenu mais par la possibilité de caractériser directement ou indirectement l'individu que la notion se décrit. Ainsi, elle élargit singulièrement la notion en ajoutant : *« an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity »*. Et le Groupe de l'article 29 créé par la directive, notamment pour interpréter la directive, devait dans une opinion importante déclarer : le Groupe de l'article 29[34] estimait que bien au-delà des données d'identité

31. Ainsi, si les noms de famille révèlent facilement l'origine ethnique, ce n'est que dans la mesure où le traitement des noms de famille entend mettre en évidence cette origine ethnique ou du moins prend en considération cette capacité de révéler une telle origine que la donnée « nom de famille » sera dite sensible. La même approche est utilisée à propos des données génétiques et biométriques, dans la mesure où la disposition ne vise que les traitements de telles données « aux fins d'identifier une personne physique de manière unique ». C'est la finalité qui justifie la spécificité de la réglementation.

32. Sur cette évolution, outre nos considérations in *La vie privée à l'heure de la société du numérique*, *op. cit.*, p. 104 s., celles de B. van der Sloot, « Do data protection rules protect the individual and should they ? An assessment of the proposed General Data Protection Regulation », *International Data Privacy Law*, 2014, 3.

33. V. à cet égard le commentaire de l'article 2 a).

34. Groupe de l'article 29, WP.136, avis 4/2007 du groupe de travail relatif au concept de donnée à caractère personnel, adopté le 20 juin 2007, p. 13. V. également les avis n^{os} 12 et 13/2011, d'une part, sur les compteurs intelligents (4 avr. 2011) et, d'autre part,

per se, le nom, l'adresse... ou par relation, le numéro de téléphone, etc., qui permettent de retrouver les données d'identité civile par l'accès à une table de connexion, des données qui permettent de repérer une personne parmi d'autres et de lui attribuer grâce à cet identifiant unique toute une série d'éléments, d'attributs ou d'actions.

Le RGPD devait reprendre la définition de la directive, tout en ajoutant des précisions sur les moyens d'identifiabilité, auxquels le responsable de traitement peut avoir recours[35]. On ajoute que la donnée même pseudonymisée, c'est-à-dire le résultat d'un traitement de pseudonymisation que l'article 4. 5) du RGPD définit comme « traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable », reste bien souvent une donnée à caractère personnel. Selon le considérant 26 du RGPD, « Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. »

La convention 108+ de 2018, si elle ne s'éloigne pas de la définition, fait un pas de plus. Le rapport explicatif affirme en effet : « Le terme "identifiable"

sur les services de géolocalisation des dispositifs mobiles intelligents (16 mai 2011). Selon le premier avis cité, le Groupe de l'article 29 distingue parmi les données à caractère personnel, trois types de données : 1. celles qui le sont par le contenu dans la mesure où celui-ci se réfère à une personne physique identifiée ou identifiable ; 2. celles qui le sont par relation, si la donnée établit un lien à un individu spécifique (par exemple, la mesure de la performance au travail d'un individu) ; 3. celles qui le sont par résultat ou par effet dans la mesure où la collecte d'un ensemble spécifique de données conduit comme effet de bord à la création d'informations à propos d'une personne identifiée ou identifiable. Ainsi une série de données de géolocalisation des voitures ou des mobiles donne de l'information à propos de leurs utilisateurs, telle que l'adresse IP.

35. Comme le notent les considérants n^{os} 26 et 30 du RGPD, « les personnes physiques peuvent se voir associer, par les appareils, applications, outils et protocoles qu'elles utilisent, des identifiants en ligne tels que des adresses IP et des témoins de connexion ("cookies") ou d'autres identifiants, par exemple des étiquettes d'identification par radiofréquence. Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes... Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci ».

ne fait pas uniquement référence à l'identité civile ou juridique en tant que telle de la personne, mais également à tout élément susceptible d'"individualiser" ou de distinguer (et donc de traiter différemment) une personne parmi d'autres. » Ainsi, on passe progressivement de l'identifiabilité à l'"individuabilité". Comme le notent très justement de Terwangne, Rosier et Losdijk à la suite du rapport explicatif de la convention n° 108 modifiée[36], on glisse dans l'interprétation de la notion de données à caractère personnel « de la notion d'identification vers un concept d'individualisation (la version anglaise utilise le terme *"singling out"* soit l'individualisation ou le ciblage)[37] ». On ajoute ensuite que la version française ne définit plus la donnée à caractère personnel comme celle « concernant » une personne déterminée mais bien, à l'instar de la version anglaise, comme une donnée se rapportant *(relating to)* à une personne déterminée. Ce changement indique bien que ce qui est premier n'est plus de savoir si la donnée est bien constitutive de l'action ou de la personne de l'individu mais simplement si elle a été ou peut être rapportée à ce dernier.

13. Faut-il arrêter là cette extension du champ d'application des législations au regard des applications les plus modernes du numérique et en particulier de l'intelligence artificielle ? Trois réflexions à ce sujet.

Les premières concernent les données anonymes. Dans la mesure où les technologies modernes de l'intelligence artificielle reposent sur de vastes réservoirs de données agrégeant tant des données anonymes que des données dites à caractère personnel et que les unes comme les autres servent à profiler des individus. Ne peut-on considérer qu'il importe d'élargir aux premières les protections réservées jusqu'à présent aux secondes ? Ainsi, si des considérations comme le revenu moyen ou le taux de mortalité à 60 ans des habitants d'un quartier, données anonymes, interviennent dans le profilage, ne faut-il pas que les personnes concernées aient connaissance de telles données et que le principe de proportionnalité leur soit appliqué[38] ?

36. C. de Terwangne, K. Rosier et B. Losdijk, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *Revue du droit des technologies de l'information*, 2016, 62, p. 6.

37. Dans le même sens, le rapport explicatif de l'article 2 de la nouvelle convention n° 108 du Conseil de l'Europe : « Le terme "identifiable" ne fait pas uniquement référence à l'identité civile ou juridique en tant que telle de la personne, mais également à tout élément susceptible d'"individualiser" ou de distinguer (et donc de traiter différemment) une personne parmi d'autres. Cette "individualisation" pourrait se faire, par exemple, à partir d'un numéro d'identification, d'un pseudonyme, de données biométriques ou génétiques, de données de localisation, d'une adresse IP ou d'un autre identifiant, qui renvoient à une personne donnée ou à un dispositif ou un ensemble de dispositifs (ordinateur, téléphone portable, appareil photo, console de jeu, etc.). »

38. La recommandation du Conseil de l'Europe sur le profilage adoptée le 3 nov. 2021 par le conseil des ministres du Conseil de l'Europe (recommandation CM/Rec(2021)8 du comité des ministres aux États membres sur la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage), reconnaît, en

Deuxième point : la distinction pourtant fondamentale et qui justifie nos législations de protection des données, entre « donnée anonyme » et « donnée à caractère personnel », tend à devenir floue. Il est loin d'être évident que l'anonymat puisse résister à l'analyse massive et croisée de quantité de données. Cette position rejoint l'interrogation des spécialistes de la technologie[39]. Ils prétendent que les croisements à l'infini de données « anonymes » de plus en plus nombreuses, croisements permis par les capacités exponentielles de nos systèmes d'information permettent de « désanonymiser » les données.

Enfin, penchés sur les opérations modernes de profilage, nous devons bien convenir que ce qui intéresse les opérateurs de *microtargeting* est non pas de cibler des individus particuliers mais bien des « groupes d'individus » fondés sur les caractéristiques que la machine définit d'ailleurs sans que, souvent, leurs utilisateurs puissent connaître de manière complète ces caractéristiques. L'individu n'est pas perçu en tant que tel mais à travers le groupe ciblé par la machine. À cet égard, ne faut-il pas envisager la protection des groupes et non seulement des individus ?

B. LES ACTEURS

14. Les législations de protection des données mentionnent de manière classique deux acteurs : d'une part, le responsable du traitement, désigné comme « maître du fichier » par la convention du Conseil de l'Europe et, d'autre part, la personne concernée. Cette conception repose sur l'idée désormais dépassée d'une relation purement bipartite entre un opérateur traitant les données et une personne physique, sujet des données traitées. L'émergence de réseaux dans lesquels circulent, se partagent et se nourrissent les données collectées grâce à mille terminaux complexifie le schéma. La directive a introduit la notion de sous-traitant, mais cette notion évoque un acteur entièrement soumis au responsable de traitement. Le RGPD (article 26) a, suite à des premières réflexions du Groupe de l'article 29 (elles-mêmes faisant suite à des jugements audacieux de la CJUE), consacré la notion de responsable

ce qui concerne ce type d'opérations, ce besoin d'extension du champ d'application de la réglementation de protection des données : « Dans le cadre de l'utilisation croissante de méga données ("big data"), des données à la fois personnelles et non personnelles sont traitées. Par ailleurs, avec des traitements automatisés, basés notamment sur l'utilisation de systèmes d'apprentissage automatique, il est difficile de savoir *a priori* quelles données permettront des corrélations ou des prédictions relatives à une personne concernée. Dans de tels cas, pour que les données à caractère personnel soient traitées de façon loyale, les organisations devraient garantir la pertinence et la qualité de toutes les données, y compris les données non personnelles, qui pourraient permettre les corrélations ou prédictions relatives à une personne concernée. »

39. À cet égard, lire notamment S. Mascetti, A. Montreale, A. Ricci et A. Gerino, « Anonymity : A Comparison between the Legal and Computer Science Perspective », *in* S. Gutwirth *et alii* (dir.), *European Data Protection Coming of Age*, Springer, 2013, p. 85 s. Ces auteurs concluent que la question de l'anonymité dépend du contexte d'usage.

conjoint, « lorsque deux responsables de traitement ou plus déterminent ensemble les finalités et les moyens du traitement ». La notion a été depuis développée tant par l'EDPB[40] que par la Cour de justice de Luxembourg. Dans l'affaire *Facebook c/ Autorité de protection belge* rendue le 15 juin 2021[41], la Cour adopte une interprétation particulièrement extensive de la notion. En l'occurrence, il était acquis que la filiale belge de Facebook ne participait en aucune manière au traitement en cause, à savoir le profilage d'un utilisateur du réseau social. Les juges de Luxembourg ont néanmoins considéré qu'il y avait responsabilité conjointe des deux entités juridiques. Certes, Facebook Belgium est chargée, à titre principal, d'entretenir des relations avec les institutions de l'Union et, à titre accessoire, de promouvoir les activités publicitaires et de marketing de son groupe, activités destinées aux personnes résidant en Belgique ; certes, le traitement principal en cause est exclusivement du ressort de Facebook Irlande. Il n'empêche, au vu de l'économie des revenus publicitaire de Facebook comme réseau social à laquelle Facebook Belgique contribue, « que dans ces conditions, les activités de l'établissement du groupe Facebook situé en Belgique doivent être considérées comme étant indissociablement liées au traitement des données à caractère personnel en cause au principal[42]... ». Ainsi, les groupes d'entreprises pourraient au regard des circonstances d'espèce être considérés comme responsables conjoints d'un traitement pourtant opéré par une filiale déterminée.

Autre exemple illustré par les arrêts *Fashion* et *Wirtschaftsakademie*[43], l'assistance donnée par des réseaux sociaux à des sites web de manière

40. EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2 sept. 2020 qui analyse les décisions déjà prises par la Cour (*Témoins de Jehovah*, C-25/27, 2018 ; *Wirtschaft Akademie Schleswig-Holstein* 5 juin 2018, C-210/16, EU : 2018:388 ; *Fashion ID c/ Verbraucherzentrale*, 29 juill. 2019, C-40/17, pts 79 s.). À noter p. 3, la synthèse des critères repris par l'EDPB : « *The GDPR introduces specific rules for joint controllers and sets a framework to govern their relationship. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. Joint participation can take the form of a common decision taken by two or more entities or result from converging decisions by two or more entities, where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing. An important criterion is that the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked. The joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand.* »

41. *Facebook Ireland, Facebook Inc., Facebook Belgium c/ APD Belgique*, 15 juin 2021, aff. C-645/19.

42. V. les attendus 92 s. On note que la décision est audacieuse dans la mesure où les juges ne réclament pas que le lien avec la finalité et les moyens soit directement établi. En l'occurrence la filiale belge contribuait indirectement par la génération de revenu à la rentabilité de l'exploitation commerciale de celui qui définissait la finalité et les moyens du traitement.

43. Décisions citées *supra* note 40.

à mieux profiler leurs visiteurs et clients[44]. Ce dernier point amène à nous interroger. Si la technologie introduit le plus souvent entre les deux acteurs traditionnels, un intermédiaire, à savoir les plateformes d'information et de communication, ne faut-il pas réglementer l'usage que ces plateformes font de cette information qui transite par elle ? La directive e-Privacy en cours de transformation ne devrait-elle pas élargir sa réglementation des traitements des opérateurs de communication à ces plateformes et ainsi limiter de façon drastique leurs utilisations possibles de l'information que leurs services de média sociaux ou d'engins de recherche génèrent[45] ?

15. Cet élargissement du nombre d'acteurs pris en compte est-il suffisant ? L'analyse de la réalité des opérations qui mènent à la mise en œuvre d'applications d'intelligence artificielle met en évidence le nombre d'acteurs qui interviennent : les fournisseurs de données, les concepteurs de (ou des) algorithme(s), les opérateurs des applications, les utilisateurs professionnels. Il est clair que la qualité des données, l'absence de biais, la sécurité du fonctionnement, l'évaluation des risques supposent sans doute une répartition des responsabilités entre tous ces acteurs mais surtout leur collaboration afin d'ajuster les paramètres, de vérifier l'adéquation et la qualité des données engrangées, etc. Il est difficile au regard du traitement qui naît de l'application retenue par un utilisateur, certes responsable du traitement, de ne pas décliner des obligations à charge de chaque membre de la chaîne des acteurs[46]. Pour certains fournisseurs d'éléments nécessaires au fonctionnement d'un système de profilage et qui les offrent commercialement sur le marché (un algorithme de base, un jeu de données nécessaires au *testing*, une base de données), devraient être requis des engagements quant à la qualité du produit, la description des limites de celui-ci et, le cas échéant, la collaboration avec le responsable dans le cadre de l'évaluation des risques et lors de la phase de tests. Même si les qualifications de responsable ou sous-traitant ne peuvent être retenues, les exigences d'une protection effective des personnes concernées plaident pour la consécration d'obligations

44. « *In terms of scope, the EDPB considers that the arrangement between targeters and social media providers should encompass all processing operations for which they are jointly responsible (i.e. which are under their joint control). By concluding an arrangement that is only superficial and incomplete, targeters and social media providers would be breach of non-compliance with their obligations under Article 26 of the GDPR.* » Sur la difficulté de tracer les limites de cette notion de « responsables conjoints » et ce à partir d'exemples concrets, lire J. Eynard, art. cité, p. 22 et 23.

45. Sur ce point, nos réflexions *in* « Les défis du profilage à l'heure de l'intelligence artificielle », dossier spécial sous la direction de C. Castets, *Rev. aff. eur.* p. 97 s.

46. V. notre description des acteurs et de leurs interactions dans le rapport Y. Poullet et B. Frenay, *Profiling and Convention 108+ : Report on developments after the adoption of Recommendation (2010)13 on profiling*, rapport établi pour le conseil consultatif de la convention n° 108, nov. 2019 dans le cadre de la révision de la recommandation de 2010 sur le profilage depuis adoptée. Le rapport est disponible sur le site du Conseil de l'Europe [https://www.coe.int/en/web/data-protection/profiling].

légales à charge d'acteurs, intervenant dans la fourniture d'algorithmes, de bases de données servant de jeux de tests ou au choix de mégadonnées, de collaborer avec le responsable du traitement pour diminuer les risques, en particulier en donnant une information sur la qualité et les limites de l'élément fourni au regard de l'objectif poursuivi par ce dernier à travers l'exploitation du système IA.

En matière d'éthique de l'IA, les recommandations de l'OCDE[47] et, plus récemment, la résolution du Parlement européen[48] plaident pour un élargissement des obligations de chaque acteur qui, de près ou de loin, participe de manière essentielle à la conception, à la mise sur pied et à l'exploitation des outils d'IA. Les fournisseurs des algorithmes ou de données doivent s'assurer de la qualité de leurs fournitures et collaborer en cas de problème avec les responsables ou sous-traitants. Enfin, cette extension de la responsabilité est au centre de la proposition de règlement sur l'IA[49] qui certes n'aborde pas en tant que telles les questions de protection des données mais inévitablement les rencontre dans la mesure où la proposition entend protéger contre les risques encourus par nos libertés du fait des applications de l'IA. Cet élargissement des acteurs à prendre en compte dans nos législations futures de protection des données est prôné par divers textes récents du Conseil de l'Europe.

47. OCDE, *Recommendation on Artificial Intelligence (AI) – the first intergovernmental standard on AI*, adoptée par le conseil des ministres de l'OCDE, le 22 mai 2019. La recommandation (p. 7) s'adresse aux acteurs de l'IA, notion définie de manière large : « Acteurs de l'IA : Les acteurs de l'IA sont les parties jouant un rôle actif dans le cycle de vie d'un système d'IA, y compris les organisations et les individus qui déploient ou exploitent l'IA ». Elle « *appelle* tous les acteurs de l'IA à promouvoir et mettre en œuvre, selon leurs rôles respectifs, les Principes suivants pour une approche responsable en appui d'une IA digne de confiance. » Même réflexion dans les *Guidelines de l'HLGE for a trustworthy IA, op. cit.*, p. 14.

48. Résolution du Parlement européen du 20 oct. 2020 *contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes*, P9_TA(2020)0275, 2020/2012/ INL, Introduction, p. 4, pt V : « Considérant que le cadre réglementaire pour l'IA de l'Union devrait englober toutes les étapes pertinentes, à savoir le développement, le déploiement et l'utilisation des technologies pertinentes et de leurs composantes, en tenant dûment compte des obligations juridiques et des principes éthiques applicables, et devrait fixer les conditions permettant de garantir que les développeurs, les « déployeurs » et les utilisateurs respectent pleinement ces obligations et principes. » Dans le même sens, p. 2, cons. 22 : « [...] estime en particulier que tous les acteurs de la chaîne de développement et d'approvisionnement des produits et des services relevant de l'intelligence artificielle devraient porter une responsabilité juridique et souligne la nécessité de mettre en place des mécanismes pour garantir la responsabilité ».

49. Proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), Bruxelles, 25 nov. 2020, COM(2020) 767 final, disponible en ligne sur [https://eur-lex.europa.eu/legal-content/FR/ALL/?uri = CELEX:52020PC0767].

C. LES « FAIR INFORMATION PRINCIPLES »

16. Le titre du chapitre n'est pas choisi au hasard même s'il est emprunté à la littérature américaine et en particulier consacré par le *Privacy Act* de 1974, qui l'applique aux seules administrations publiques. C'est que dès les résolutions de 1973 et 1974, le Conseil de l'Europe les a repris à son tour et que ces principes continuent à être la pierre angulaire de nos législations de protection des données. Reprenons-les tels qu'énoncés par la convention de 1981 : « Les données à caractère personnel faisant l'objet d'un traitement automatisé sont : a) obtenues et traitées loyalement et licitement ; b) enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités ; c) adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées ; d) exactes et si nécessaire mises à jour ; e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées. » Sans être modifié, le principe de « finalité légitime » a été précisé par la directive de 1995 en énumérant une liste exhaustive de fondements de légitimité, conditions nécessaires mais non suffisantes de légitimité, parmi lesquelles première citée, le consentement, jusque-là jamais mentionné comme cause de légitimité. On ajoutera que l'article 8.2 de la Charte déjà citée[50] donne à ce fondement une place particulière *sui generis* : « Ces données doivent être traitées loyalement, à des fins déterminées et sur base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. » Sans vouloir commenter pour l'instant ce que d'aucuns considèrent comme un « *privacy bug*[51] », notons que le dogme du consentement est fondé sur l'argument simple suivant et en apparence imparable : le consentement n'offre-t-il pas à la personne concernée la meilleure des protections, puisqu'il fait dépendre de notre bon vouloir dûment informé, libre et spécifique, le traitement par autrui de nos données à caractère personnel, devenu comme

50. Le même texte a été introduit dans la convention 108+ lors de son adoption en 2018. Un article 5.2 a été ajouté : « Chaque Partie prévoit que le traitement de données ne peut être effectué que sur la base du consentement libre, spécifique, éclairé et non-équivoque de la personne concernée ou en vertu d'autres fondements légitimes prévus par la loi. » On note cependant que ce point est précédé d'un point 5.1 également ajouté qui rappelle que le principe de proportionnalité s'impose même en cas de consentement : « Le traitement de données doit être proportionné à la finalité légitime poursuivie et refléter à chaque étape du traitement un juste équilibre entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu. »

51. Comme l'écrivent M^mes^ Lobet et Cohen (C. Lobet-Maris, « Le fétichisme de la donnée à caractère personnel. Relecture politique et critique de la vie privée », *in* E. Degrave *et alii* [dir.], *Law, Norms and Freedoms in the Cyberspace. Liber Amicorum Y. Poullet*, *op. cit.*, p. 696 et J. Cohen, « Privacy, Ideology and Technology », *Georgetown Law Journal* 2011, 89, p. 2029). De manière plus nuancée mais également critique, J. Eynard, « "Empouvoirement" individuel », *in* dossier spécial sous la direction de C. Castets, *Rev. aff. eur.* 2021, n° 1, p. 21 s.

« notre » propriété ? N'est-il pas, par ailleurs, l'expression la plus achevée de notre autonomie ou auto-détermination, concept qui définit la vie privée consacrée par l'article 8 de la Convention européenne des droits de l'homme sur lequel s'appuient les législations de protection des données ? Le RGPD ajoute à la liste des principes de base la sécurité (article 6.1.f) et celui d'*accountability* (article 6.2.), suivant lequel le responsable du traitement est responsable du respect de l'ensemble des « *Fair Information Principles*[52] » et a pris les mesures nécessaires à cet effet. Ce dernier point renvoie à diverses mesures de « *compliance* » interne : ainsi, pour ne citer que certaines : la rédaction d'une *Privacy Policy* (article 24.2), la nomination d'un délégué à la protection des données (article 37 s.) et, à propos de certains traitements à risque, celui d'une évaluation de l'impact des traitements en cause sur les personnes concernées (article 35 et 36).

17. Toutes ces mesures illustrent la montée de ce que M^me^ Frison-Roche[53] appelle le droit de la *compliance* et ce, dans un domaine non plus sectoriel comme c'est le cas dans des secteurs comme les banques, les télécommunications, l'énergie, mais cette fois vis-à-vis d'une thématique horizontale. En d'autres termes, c'est à l'intérieur des entreprises et, en tout cas, avec leur plein appui individuel ou collectif[54], qu'est recherchée cette effectivité. Appelés à être de « *good corporate citizens* »[55] », les responsables de traitement deviennent les premiers agents du respect des prescrits. Comme l'écrit Frison-Roche[56], « dans le même temps que le droit de la compliance consiste à internaliser le droit de la régulation dans les entreprises en position de rendre mondialement effectif celui-ci, le droit de la compliance assure cette effectivité en contrôlant la mise en œuvre : il instaure en même temps la supervision de ces entreprises cruciales par les autorités de régulation. C'est ainsi qu'un nouveau continuum révolutionnaire s'est mis en place entre régulation, supervision, compliance ». Une autre évolution mérite d'être notée. Ces mesures sont dictées par la prise de conscience que la mise en œuvre de certains

52. On note que ce principe est repris des lignes directrices de l'OCDE. L'article 24.1. du RGPD explicite la règle : « Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met 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. Ces mesures sont réexaminées et actualisées si nécessaire. »

53. M.-A. Frison-Roche, « Du droit de la régulation au droit de la compliance », *in* M.-A. Frison-Roche (dir.), *Régulation, supervision, compliance*, Dalloz, 2017, p. 1 s.

54. Ainsi par l'adoption de codes de conduite propres à une communauté ou association d'entreprises ou de mécanismes de labellisation ou de certification.

55. L'expression est de B. de Juvigny, « La compliance, bras armé de la régulation », *in* M.-A. Frison-Roche (dir.), *Régulation, supervision et compliance*, Dalloz, coll. « Thèmes & commentaires », série « Régulations », 2017, p. 17.

56. M.-A. Frison-Roche, « Du droit de la régulation au droit à la compliance », in *Régulation, supervision et compliance*, *op. cit.*, p. 1 à 14.

traitements engendre des risques particuliers pour nos libertés individuelles. Au système mis en place par la Directive consistant en des formalités administratives imposées à tous les traitements : à savoir la notification préalable aux autorités de contrôle, le RGPD[57], à la suite des considérations du Groupe de l'article 29[58], substitue une approche procédurale fondée sur la gravité des risques liés à certains traitements[59]. Cette approche, centrée sur le risque et la mise en place de procédures pour évaluer et diminuer ce risque, rejoint celle suivie par la Commission européenne dans sa proposition de règlement sur l'IA. Elle apparaît plus conforme au principe de proportionnalité et repose sur une confiance bien nécessaire dans les acteurs de la société du numérique. La proposition de la Commission cherche en effet à établir un compromis entre les exigences légales et éthiques, traduisant les valeurs de l'Union, et la nécessité de ne pas contraindre de manière exagérée le développement et l'initiative technologiques[60]. Pour ce faire, le texte adopte une approche règlementaire strictement proportionnée, évolutive, fondée sur la distinction entre pratiques illégales de l'intelligence artificielle[61] (art. 5), systèmes d'IA à haut risque (art. 6.2) et les autres. La proposition oblige par ailleurs les opérateurs de systèmes IA à prendre toute une série de mesures internes afin de veiller à la gouvernance de tels systèmes dès le stade de la conception, à leur évaluation et à leur gestion continue. On notera que l'opinion de l'EDPB et de l'EDPS à propos de cette *« risk based approach*[62] » est particulièrement enthousiaste même si ces instances auraient souhaité un élargissement des catégories de traitements présentant un risque inacceptable

57. V. le considérant n° 89 du RGPD : « Ces obligations générales de notification sans distinction devraient dès lors être supprimées et remplacées par des procédures et des mécanismes efficaces ciblant plutôt les types d'opérations de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, du fait de leur nature, de leur portée, de leur contexte et de leurs finalités. » Sur cette évolution d'approche, lire N. Metallinos, « Des formalités préalables aux études d'impact sur la vie privée (ELVP) », *CCE* 2018. Dossier 1.

58. Groupe de l'article 29, avis n° 3/2010, sur le principe de la responsabilité, 13 juill. 2010, WP. 173.

59. Dans le même sens, l'article 11 de la convention n° 108 + : « Chaque Partie peut, eu égard aux risques encourus pour les intérêts, droits et libertés fondamentales des personnes concernées, adapter l'application des dispositions des paragraphes 1, 2 et 3 dans la loi donnant effet aux dispositions de la présente Convention, en fonction de la nature et du volume des données, de la nature, de la portée et de la finalité du traitement et, le cas échéant, de la taille des responsables du traitement et des sous-traitants. »

60. Pour plus de détails sur cette proposition, lire Y. Poullet, « Vers un droit européen de l'intelligence artificielle », *Journal de droit européen*, Larcier, n° 284, 2021, p. 454-463.

61. Ainsi, les systèmes de manipulation par messages subliminaux, l'exploitation des vulnérabilités, l'utilisation par le secteur public de systèmes de *« social ranking »* entraînant de potentielles discriminations entre personnes ou groupes, de systèmes biométriques fonctionnant en temps réel et à distance, placés dans des endroits publics (par exemple, des systèmes de reconnaissance faciale...).

62. EDPB-EDPS, Joint opinion 5/2021 on the proposal for a regulation of the EU Parliament and of the Council laying down harmonised rules on AI, June 18, 2021.

ou un haut degré de risques : « The EDPB and the EDPS *welcome the risk-based approach* underpinning the Proposal. However, this approach should be clarified and the concept of "risk to fundamental rights" aligned with the GDPR and the Regulation (EU) 2018/1725 (EUDPR), since aspects related to the protection of personal data come into play. »

18. L'irruption des techniques d'intelligence artificielle fondées sur le *machine learning* soulève de nouvelles questions quant à l'applicabilité des *Fair Information Principles*[63]. La première concerne la détermination des finalités. La richesse possible des agrégations permise par les algorithmes au sein des *big data* voire l'évolution de celles-ci, en fonction de nouvelles données collectées, permet à l'exploitant du système d'entrevoir de nouvelles applications possibles. Ainsi, le profilage de la clientèle peut, dans un premier temps, avoir pour seule finalité la sélection de celle-ci, l'affinement du système peut amener à avoir une meilleure connaissance des potentiels clients ainsi sélectionnables et sur cette base de leur proposer des prix différenciés en fonction d'indices de leur demande potentielle pour tel ou tel produit[64]. On notera que les capacités prédictives de l'outil peuvent amener à interdire *a priori* certaines finalités[65] ou à entourer leur poursuite de précautions procédurales et d'évaluation externe particulières[66].

Les principes de minimisation et de proportionnalité de la durée rencontrent également des difficultés d'application dans le cadre des traitements utilisant des systèmes d'IA. Ces principes présupposent que l'on

63. Sur cette applicabilité difficile des principes énumérés par l'article 5 du RGPD, lire notre étude, *Le RGPD face aux défis de l'intelligence artificielle*, Cahier du CRIDS, n° 48, Bruxelles, Larcier, en particulier p. 64 à 83.

64. Les données de géolocalisation reprises par Google servent à des finalités multiples, en dehors de celles poursuivies par le responsable lui-même, soit à des clients professionnels de Google, intéressés par l'envoi de publicités ciblées à des personnes proches des lieux où ils offrent leurs biens ou produits, soit demain à des autorités publiques municipales préoccupées par un meilleur planning urbain dans le cadre de leur lutte contre la pollution ou pour signaler des alternatives de mobilité à leurs citoyens.

65. On retrouve là les interdictions listées par la proposition d'Artificial Intelligence Act, tels le *social credit scoring* ou certaines applications de reconnaissance faciale. Autre exemple : l'article 4.2 de la loi belge sur les assurances, modifiée le 4 déc. 2020, prévoit : « Lors de la conclusion du contrat visé à l'article 46/1, le refus du candidat assuré d'acquérir ou d'utiliser un objet connecté qui récolte des données à caractère personnel concernant son mode de vie ou sa santé ne peut en aucun cas conduire à un refus d'assurance ni à une augmentation du coût du produit d'assurance. » Et l'article 5 introduit un article 46.3 qui énonce : « Aucune segmentation ne peut être opérée sur le plan de l'acceptation, de la tarification et/ou de l'étendue de la garantie sur la base de la condition que le candidat assuré accepte d'acquérir ou d'utiliser un objet connecté qui récolte des données à caractère personnel concernant son mode de vie ou sa santé, accepte de partager des informations récoltées par un tel objet connecté, ni sur la base de l'utilisation par l'assureur de telles informations. »

66. On pense ici à la proposition de règlement Digital Service ACT qui obligerait les *« very large »* plateformes de faire auditer leurs algorithmes relatifs à leurs systèmes de recommandation par des sociétés tierces et de suivre les recommandations de ces dernières.

puisse *a priori* déduire de la finalité de l'application les données nécessaires à son obtention et la durée de leur conservation. Or les systèmes dits de *machine learning* fonctionnent grâce à des corrélations statistiques établies sur la base de rapprochements souvent non prévisibles de données et exigent donc que les réservoirs de données brassent très largement[67]. Le projet de recommandation du Conseil de l'Europe sur le profilage, déjà cité, en son point 3.2. au nom de ces principes, recommande au moins la balise des *« legitimate expectations »* : « Les données personnelles utilisées dans le cadre du profilage devraient être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles seront traitées. Dans les systèmes de *"machine learning"* il est difficile de connaître *a priori* quelles données permettront des corrélations significatives. Par ailleurs, il est important de limiter le traitement de profilage à des catégories de données dont la personne concernée peut raisonnablement s'attendre (légitimement s'attendre) à ce qu'elles soient prises en considération au vu des finalités du profilage. » Sans doute cette balise est-elle insuffisante et faudra-t-il, secteur par secteur avec le cas échéant une intervention législative fixant elle-même certaines limites aux données utilisées, répondre à des questions, qui sont loin d'être triviales comme les suivantes : « Jusqu'où une compagnie d'assurances peut-elle utiliser des données relatives aux personnes assurées dans le cadre de l'offre de services individualisés ? » ; « Jusqu'où une banque ou un organisme de crédit peuvent-ils, au nom de leur responsabilité de donneur de crédit et suivant les exigences du principe *"Know your customer"*, profiler ses clients ? » ; « Dans quelle mesure, un employeur peut-il utiliser, vis-à-vis des employés ou candidats employés, des systèmes d'*affective computing* dans le cadre de leur sélection, gestion de carrière, etc. ? »

19. On ajoutera que la généralisation des systèmes d'IA dans le cadre de prises de décision amène à affirmer avec force un principe supplémentaire introduit par la Directive (article 15) mais désormais consacré par le RGPD, même si insuffisamment, nous semble-t-il. L'article 22 du RGPD, consacrant le droit de la personne concernée « de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire », appelle les remarques suivantes. L'analyse de cette disposition laisse apparaître nombre de lacunes ou, en tout cas, d'ambiguïtés. Que veulent dire les expressions : « décision fondée exclusivement » ;

67. Ainsi, hypothèse purement fictive, il pourrait apparaître, aux yeux de l'administration fiscale, lors de l'utilisation de vastes banques de données, que les dirigeants d'entreprise de plus de 200 employés et moins de 400, disposant d'une voiture rouge immatriculée entre telle et telle année, ayant l'habitude de voyages *« all inclusive »* dans les pays méditerranéens, habitant tel type de quartier dans des villes de plus de 50 000 habitants, avec un enfant et un chien, constituent des fraudeurs potentiels. Cet exemple témoigne du fait qu'il est difficile, *a priori* du moins, de fixer les éléments qui serviront à établir le profil.

« affecter de manière significative » et le terme « uniquement » ? Enfin, la décision évoquée par l'article 22 doit viser une « personne concernée ». C'est la conséquence certes d'une législation centrée sur la protection de personnes individuelles mais ne faudrait-il pas également prendre en compte le fait que des systèmes en particulier prédictifs visent des catégories de personnes : ainsi les personnes habitant tel quartier, ayant tel type de comportement sur le Net, telle mobilité, tel bagage génétique... ? Le risque est ici collectif et, de ce fait, mériterait *a fortiori* d'être pris en compte. Nous ne pourrons dans le cadre de cette contribution analyser toutes ces ambiguïtés[68]. Par ailleurs, l'article 22.2 prévoit des exceptions qui s'appliqueront à la plupart des systèmes d'IA : besoins contractuels ou précontractuels, consentement de la personne concernée ou exécution d'une mission d'intérêt public autorisée par l'État. Manque l'hypothèse d'un système IA dont la licéité reposerait sur un intérêt légitime prépondérant du responsable du traitement. Dans de tels cas, la disposition évoque simplement le droit à des « mesures appropriées » et à l'obtention d'une intervention humaine, sans oser affirmer un droit à l'explication qui s'ajouterait au droit à l'information. Certes, l'intervention humaine ne peut se limiter à une simple réaffirmation par oral de la « vérité sortie de l'ordinateur » mais à partir de quand pourra-t-on considérer que l'humain a une réelle capacité de remise en cause de la présomption de vérité sortie des ordinateurs[69] et ce d'autant plus que le système (voir les systèmes dits de *deep learning*) fonctionne de manière partiellement opaque ? Que recouvrent les termes *« garanties appropriées »* : le droit à une audience en face à face ? Un droit de contestation de la décision après explication ? On note que ce thème que nous avons rangé sous l'angle des principes eut pu être abordé sous l'angle des droits subjectifs de la personne concernée. Il est vrai, comme le note J. Eynard[70], que « telles les deux faces d'une même pièce, aux droits conférés à la personne concernée répondent les obligations imposées au responsable de traitement ».

68. Sur cette analyse, nous renvoyons à notre ouvrage : *Le RGPD face aux défis de l'intelligence artificielle*, Cahier du CRID, n° 48, Bruxelles, Larcier, 2020, p. 109 s., n^os^ 35 s. ; et les différentes références y reprises.

69. Sur cette « incontestabilité » de la décision produite par la machine, lire entre autres, M. Kaminsky : *« And where human decision-making can often be contested, algorithmic decision-making [...] is often taken at face value, and left unchallenged and unchallengeable »* (« Binary governance : lessons from the GDPR's approach to algorithmic accountability », *Southern California Law Review* 2019, 76, p. 15). Il semble que les autorités singapouriennes exigent que les personnes chargées de répondre aux demandes d'explication ou de contestation des décisions d'applications de *« machine learning »* disposent d'une réelle compétence en matière de *machine learning* et connaissent l'application.

70. J. Eynard, art. cité, p. 22.

III. LA MONTÉE DES DROITS SUBJECTIFS DE LA PERSONNE CONCERNÉE

20. Comme le pointe très justement B. van der Sloot[71], c'est certainement du côté des prérogatives des personnes concernées que les évolutions législatives les plus importantes sont à constater. En quelques mots, on note que l'article 6 de la résolution de 1974 du Conseil de l'Europe relative à la protection des données dans le secteur privé ne reconnaissait à la personne concernée qu'un droit à l'information relative aux données conservées à son propos, la finalité de cette conservation et les communications à des tiers.

La convention du même Conseil de l'Europe en son article 8 ajoute une série de droits subjectifs au bénéfice de la personne concernée : outre le droit de connaître l'existence des traitements opérés à son propos, leur finalité et les destinataires de la communication des telles données, le droit de se faire communiquer les données la concernant dans un format intelligible, celui de rectification en cas d'erreur ou de violation des principes, de même que le droit au recours et de dédommagement en cas de refus d'obtempérer de la part du « maître du fichier ».

La directive complète la liste par la reconnaissance (article 12) d'un droit d'accès large et gratuit aux données traitées et aux résultats de ce traitement (qui ? quoi ? et pourquoi ?...). Le droit de rectification se précise en un droit de radiation ou de blocage de la donnée en cas de non-respect des principes et obligations du responsable de traitement et s'ajoute enfin le droit de refuser le traitement de données dans certains cas limités (marketing et prépondérance d'un intérêt particulier personnel sur l'intérêt légitime du responsable de traitement). Enfin, le point a déjà été évoqué lors de l'analyse des principes : le droit de ne pas être soumis à une décision automatisée.

Le texte de la Charte érige le droit d'accès en élément du droit fondamental à la protection des données[72]. À cette liste devenue longue, le RGPD ajoute

71. B. van der Sloot, « Do data protection rules protect the individual and should they ? An assessment of the proposed General Data Protection Regulation », *International Data Privacy Law* 2014, 3.

72. V. l'interprétation donnée par la CJUE dans son arrêt du 14 juill. 2014 (affaires C-141/12 et 372/12) : « L'article 12, sous a), de la directive 95/46 et l'article 8, paragraphe 2, de la charte des droits fondamentaux de l'Union européenne doivent être interprétés en ce sens que le demandeur d'un titre de séjour dispose d'un droit d'accès à l'ensemble des données à caractère personnel le concernant qui font l'objet d'un traitement par les autorités administratives nationales au sens de l'article 2, sous b), de cette directive. Pour qu'il soit satisfait à ce droit, il suffit que ce demandeur soit mis en possession d'un aperçu complet de ces données sous une forme intelligible, c'est-à-dire une forme permettant à ce demandeur de prendre connaissance desdites données et de vérifier que ces dernières sont exactes et traitées de manière conforme à cette directive, afin que ledit demandeur puisse, le cas échéant, exercer les droits qui lui sont conférés par ladite directive. »

encore quelques compléments et non des moindres[73] : ainsi la possibilité pour la personne concernée d'utiliser les outils numériques pour l'accès à ses données ou pour l'exercice de ses droits, selon un principe sain de partage des bénéfices, à savoir que, si la technologie bénéficie au responsable du traitement pour ces opérations de traitement, il est normal que le même outil puisse servir à la personne concernée dans l'exercice de ses droits ; ainsi, le droit à la portabilité (article 20) des données, qui permet à la personne concernée d'obtenir les données (uniquement celles qu'elle a fournies, pas celles obtenus de tiers ni celles produites par les traitements du responsable ou de tiers !) et de pouvoir dès lors les confier à un autre responsable de traitement[74].

Le RGPD introduit le droit à la connaissance des incidents de sécurité qui ont conduit à la violation des données (article 34). Il consacre les droits à l'oubli (article 17) et à la limitation du traitement (article 18) qui élargissent ou modalisent l'ancien droit à la rectification et au blocage de la directive et surtout bénéficient d'un renversement de la charge de la preuve : désormais, principe d'*accountability* oblige, c'est, en cas de contestation, au responsable du traitement à faire la preuve de son respect des obligations et des principes. Enfin, l'article 80 permet la représentation des personnes concernées par un organisme mandataire de leurs intérêts individuels voire même sans mandat pour les pays qui reconnaissent à ces organismes un droit d'action propre. On note que cette possibilité permet de conclure à une quasi « action collective » même si elle est liée à la démonstration d'une violation du droit individuel d'une ou de plusieurs personnes concernées.

21. Cette reconnaissance élargie de droits subjectifs à la personne concernée, consacrée par une modification de l'article 1 de la loi « Informatique et libertés » : « toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant », part du postulat que c'est la personne concernée elle-même qui, par son exercice et sous le contrôle (ou avec l'aide) des autorités de protection des données, est le mieux à même de contrôler l'usage qui est fait de ses données et ainsi de faire respecter les principes et les obligations du responsable du traitement. Cette conviction pose problème à l'heure où, d'une part, le déséquilibre informationnel entre les personnes concernées et les responsables de traitement, du moins certains, devient abyssal et, d'autre part, où les enjeux des traitements sont de plus en plus collectifs voire concernent la société en tant que telle. Ces critiques nous apparaissent fondamentales et justifient

73. On mentionne, parmi les ajouts non significatifs, quelques informations dues par le responsable du traitement : la durée du traitement, le nom du détaché, la logique du traitement en cas de profilage, etc.

74. Cette disposition relève autant du droit de la concurrence que du droit de la protection de ces données. Il n'empêche qu'il accroît la maîtrise par les personnes concernées de leurs données.

notre crainte de voir le consentement présenté comme le paradigme même de l'« empouvoirement » des personnes concernées et la base par excellence de la légitimité des traitements.

22. Avant d'entamer cet examen, notons que le consentement comme base de légitimité des traitements n'a été affirmé explicitement qu'avec la directive de 1995. Les premiers textes n'en font pas mention et, sans doute, sont-ce les attendus célèbres de l'arrêt du tribunal constitutionnel rappelé ci-dessus[75], consacrant le principe d'autodétermination informationnelle, qui explique cette insertion. La directive prend soin d'exiger un consentement libre, informé et spécifique[76] ; le RGPD ajoute que la manifestation de volonté doit être univoque, que le consentement (article 7) est rétractable et ne peut être une condition « superflue » de l'exécution d'un contrat. Ces exigences prises au sérieux devraient conduire à exclure le consentement de la plupart des traitements tant publics que privés. Le consentement n'existe que si la personne concernée dispose d'un réel choix entre diverses options et que le refus de consentir n'entraîne pas un préjudice. On peut ainsi considérer que certains contextes[77] ou le statut « vulnérables » de certaines personnes concernées[78] rendent invalides le consentement. La complexité des montages des systèmes supportés par les technologies de l'IA, la diversité des sources utilisées, l'impossibilité de prévoir les corrélations qui seront à la base des décisions du responsable et, dans le contexte de l'accès à des services gratuits et à portée d'un clic, la difficulté de prendre le recul nécessaire au moment où on clique sur le « j'accepte », tous ces facteurs rendent les conditions mises par le RGPD complètement illusoires d'autant plus que le refus conduit à un non-accès au service[79]. Dans de telles conditions, le consentement ne peut être, sauf exceptions, la condition d'accès à des services souvent ressentis comme nécessaires à l'exercice de la vie sociale.

75. V. l'arrêt cité note 9.

76. Groupe de travail de l'article 29, « Lignes directrices sur le consentement au sens du règlement 2016/679 », adoptées le 28 nov. 2017, version révisée et adoptée le 10 avr. 2018.

77. Ainsi, le consentement obtenu lors d'une visite d'un site web en ce qui concerne l'acceptation de traitements permis par des cookies, selon la formule souvent trompeuse à moins qu'elle ne soit ironique, des opérateurs de ces sites : « Nous sommes soucieux de votre vie privée. » Ce consentement via cookies interposés sera obtenu de manière globale ou à travers un paramétrage fastidieux et souvent aux critères incompréhensibles de vos préférences.

78. Ainsi, le travailleur, le candidat à un emploi ou le malade...

79. À cet égard, les craintes exprimées par le Parlement européen dans sa résolution du 25 mars 2021 concernant le rapport d'évaluation de la commission sur la mise en œuvre du RGPD deux ans après son entrée en application (2020, 2717 [RSP], P 9, T. A. [2021]0111, p. 6) : « [le Parlement est] préoccupé par le fait que les personnes subissent souvent une pression financière qui prend la forme d'une invitation à donner son consentement en contrepartie de ristournes ou d'autres offres commerciales, ou qu'elles sont contraintes par des clauses de prestation subordonnée à donner leur consentement si elles veulent avoir accès à un service ».

Que proposer dès lors ? Sans doute, et ces solutions ont notre préférence, faut-il prescrire, là où c'est possible et suivant l'exemple du droit de la consommation, un consentement collectif négocié entre le responsable du traitement et les représentants des usagers (avec ou sans la médiation des autorités de protection des données). Sans doute, faut-il, dans certains cas, interdire en principe le consentement, et réclamer que seules les autres causes de validité soient invocables[80], qu'il s'agisse tantôt de la nécessité d'exécution d'un contrat ou des mesures précontractuelles, tantôt de l'intérêt légitime de l'opérateur qui trouvera des justifications supplémentaires au traitement dans les trois apports présumés de l'IA : la sécurisation, l'optimisation et l'objectivation. À défaut, ne faut-il pas laisser le choix à la personne concernée entre un accès non profilé et un accès profilé, voire entre un accès anonyme ou au contraire identifié[81] ? Au-delà, il importe que la personne concernée puisse dans certains cas de traitements fondés sur des systèmes d'intelligence artificielle, en particulier lorsqu'il s'agit de profilage à des fins publicitaires[82], définir la finalité du profilage qu'elle souhaite et, dès lors, réduire le champ des données qui seront exploitées.

80. À cet égard, les réflexions de J. Eynard (art. cité, p. 21) et de E. Deraedts, « À propos des dérives actuelles du consentement en matière de protection des données », *AJDA* 2021. 346, invoquant leurs craintes de voir, y compris dans le cas de traitements par l'autorité publique, un réel « moyen de contournement d'une légalité plus stricte ».

81. On reprendra volontiers sur ces deux points (droit à l'anonymat et droit à ne pas être profilé), la recommandation 3.8 du projet du Conseil de l'Europe relatif au profilage, qui affirme : « Dans toute la mesure du possible, les prestataires de services et les plateformes devraient offrir différents services plus ou moins personnalisés, voire non personnalisés, en fonction du service offert, afin de garantir que la personne concernée ait le choix en ce qui concerne l'intensité du profilage. Pour qu'il soit libre, le consentement suppose pour le moins, pour la personne concernée, la possibilité d'un choix informé. Le consentement au profilage ne devrait pas pouvoir être exigé comme condition de la prestation d'un service. Quand le consentement est requis, il incombe au responsable du traitement de prouver que la personne concernée a accepté explicitement le profilage au-delà de ce qui était nécessaire à l'exécution de la prestation et ce après avoir été informée... »

82. Prenons un exemple, l'accès à un service de musique en ligne ne suppose pas que vous soyez d'accord avec le profilage de vos goûts musicaux lequel, en revanche, est nécessaire si vous souhaitez que le fournisseur vous conseille ou vous propose des musiques adaptées à vos goûts. Votre choix devrait pouvoir porter sur chacune des diverses finalités et, le cas échéant, sur les destinataires tiers qui permettront de réaliser les finalités. Ainsi, pour reprendre toujours l'exemple du service de musique en ligne, peut-être, le souhait de l'internaute est-il de recevoir l'annonce publicitaire émanant de tiers à propos de la sortie d'une chanson de son interprète favori ? À l'inverse, le choix de l'internaute peut s'exprimer en sens contraire. En d'autres termes, admettre le profilage à des fins publicitaires par le responsable de traitement ne signifie pas nécessairement admettre le profilage par des tiers ou la cession de données ou de mon profil à des tiers. Autre exemple, l'utilisation de systèmes d'IA dans le cas de voitures connectées devrait distinguer les hypothèses où le possesseur de la voiture connectée souhaite connaître son profil de conducteur à des fins personnelles (respect des limites, analyse de la consommation, risques pris – par exemple : conduite en état de somnolence ou d'alcoolisme...) sans que ces « profils » ne soient accessibles à son garagiste hormis pour des raisons de sécurité, de l'hypothèse où ce possesseur refuse l'utilisation de tout système d'IA...

23. De manière plus fondamentale, ne peut-on considérer que le consentement met la personne concernée au centre de la responsabilité de la protection des données et lui donne l'illusion d'une maîtrise de la « propriété » de ses données[83] alors même qu'il n'en est rien. Par ailleurs, peut-on faire dépendre la légitimité d'un traitement d'un consentement individuel qui certes poursuit l'intérêt de la personne consentante mais risque de préjudicier aux autres ? Faut-il se limiter à l'examen de la seule sphère relationnelle entre la personne concernée et soit son contractant, soit le responsable ou les responsables du traitement ou faut-il introduire une dimension plus collective ? De manière plus explicite, une personne souscrit un contrat d'assurance prévoyant une diminution importante de ses primes sous la condition d'une surveillance en continu de sa conduite, il va de soi que la nécessité du contrat accepté par le preneur d'assurance implique le traitement des données de conduite automobile de la personne concernée. Juge-t-on pour autant que le traitement est licite ? En principe oui, puisqu'objet d'un contrat, mais ne peut-on objecter que ce système met en cause le principe de mutualisation qui gouverne notre conception de l'assurance[84] ? Sans doute, cette remarque renvoie à la dimension collective et sociétale du débat « Vie privée », dimension qui, nous l'avons dit (*supra*, n° 9, *in fine*), est obscurcie par la dimension purement individualiste de nos législations Vie privée.

IV. DES AUTORITÉS DE PROTECTION DES DONNÉES ET DE LA QUESTION DES EFFETS TRANSFRONTIÈRES DE NOS LÉGISLATIONS EUROPÉENNES

24. En 1987, D. Flaherty, alors commissaire à la protection de la vie privée au Canada, opposait deux visions du futur des commissions de protection de la vie privée. L'une les décrivait comme des « chiens de garde », sans autre compétence que de dénoncer les dangers encourus par notre vie privée. L'autre l'envisageait comme une autorité administrative chargée certes de rendre justice mais également et surtout de veiller au respect des contraintes administratives imposées par les législations. La crainte de l'auteur était de

83. Sur cette analyse de la protection des données comme propriété et les critiques sévères à adresser à cette analyse, lire Y. Poullet, « Consent : the Privacy bug », *in* A. Giudicelli et E. A. Caprioli (dir.), *La confiance numérique. Travaux de la Chaire sur la confiance numérique*, LexisNexis, 2022, p. 97 s.

84. Un autre exemple, peut-on admettre, comme Amazon le prétend, que l'intérêt de la personne concernée est d'obtenir une publicité *ad hoc* en fonction de ses choix précédents et de la connaissance qu'Amazon a de ses clients futurs ou présents et dès lors justifier le traitement de telles données sur base de l'article 6 f) sans que pour autant ce ne soit nécessaire à l'exécution du contrat et pourrait porter atteinte à la dignité de la personne.

voir le second rôle faire oublier le premier. L'histoire législative de la protection des données témoigne d'un rôle et d'une compétence accrus des organes mis en place pour assurer la protection des données, sans que pour autant ceux-ci ne perdent leur âme. La création de tels organes est le fait de législations dites de première génération, la première (1973), celle suédoise ; la seconde (1977), celle allemande et finalement en 1978, celle française : la CNIL. Indiscutablement, la législation française se distinguait de la plupart de celles des autres pays par la compétence importante confiée à cette autorité à la fois administrative et indépendante. L'article 6 de la loi mentionnait alors : « Une commission nationale de l'informatique et des libertés est instituée. Elle est chargée de veiller au respect des dispositions de la présente loi, notamment en informant toutes les personnes concernées de leurs droits et obligations, en se concertant avec elles et en contrôlant les applications de l'informatique aux traitements des informations nominatives. La commission dispose à cet effet d'un pouvoir réglementaire, dans les cas prévus par la présente loi. » L'article 13 de la convention n° 108 se contente de mentionner l'obligation pour chaque partie à la convention de désigner une (ou plusieurs) autorité(s) sans préciser les compétences à lui (leur) attribuer si ce n'est celle de coopérer entre elles au profit des personnes concernées non résidentes sur le territoire. L'article 28 de la directive européenne de 1995 réclame l'indépendance de ces autorités, et fixe leurs compétences : compétence nécessaire d'avis sur toutes mesures réglementaires ou administratives relatives à la protection des données ; compétences minimales d'investigation et d'ester en justice. La saisine de l'autorité par toute personne concernée ou association représentant cette dernière est consacrée. La présence d'une autorité de contrôle constitue désormais un élément du droit fondamental de la protection des données. L'article 8.3 de la Charte en fait l'instrument privilégié du contrôle du respect des règles de législation de protection des données. Pour répondre à cet objectif, le RGPD affirme, à la suite de divers arrêts de la CJUE, le principe de l'indépendance de cette autorité (article 51 s.) et accroît encore ces compétences (articles 55 s.). Le RGPD liste ainsi pas moins de 22 chefs de compétence, en particulier énumère longuement les pouvoirs d'enquête et surtout de décision (y compris l'octroi de sanctions administratives), pouvoirs bien évidemment soumis à un contrôle juridictionnel.

25. La dimension collaborative du travail des autorités de protection des données mérite d'être soulignée. Dès la convention n° 108, la coopération entre parties à la convention était exigée (article 13) à travers des autorités désignées par chaque État, chargées dans ce contexte tantôt d'informer de l'état de la législation et du traitement automatisé mis en cause par l'autorité correspondante dans l'État d'origine de la plainte, tantôt d'assister la personne concernée, résidant à l'étranger et ayant présenté sa demande via l'autorité du pays de la résidence. La volonté d'introduire un marché commun de la

donnée à caractère personnel devait amener la directive à aller plus loin dans cette exigence de coopération et ce par la création du Groupe dit de l'article 29 composé d'un seul représentant par État membre de l'autorité ou des autorités nationales de protection des données. Les compétences de ce groupe sont nombreuses (article 30) : outre les compétences consultatives et, en particulier, d'examen des dispositions nationales au regard de la directive, ce qui devait donner lieu aux nombreuses opinions et avis comme autant de précisions parfois hardies apportées au texte de la directive, le groupe avait pour tâche de prévenir tout différend d'interprétation de la directive et d'émettre des recommandations sur toute question concernant la protection des données, en particulier sur des innovations technologiques.

Le RGPD devait franchir un pas supplémentaire. Le principe d'assistance mutuelle est consacré (article 61) et renforcé notamment par la possibilité d'actions conjointes (article 62). La volonté d'une interprétation et d'une application uniforme explique cette progression. Les dispositions du RGPD prennent soin tout d'abord de préciser les modes de collaboration des autorités de protection des données, en fixant à la fois le chef de file en cas de litiges selon le critère du lieu d'établissement principal du responsable du traitement mais également ses devoirs de coopération dans le cadre de la procédure dite IMI *(Internal Market Information System)*, qui oblige le chef de file à consulter toutes les autres « autorités concernées » (article 4, § 22) du fait de l'existence du traitement.

Ce système de « guichet unique », et d'une autorité « chef de file », coordinateur plutôt qu'unique décideur, est remis en cause tantôt par certaines autorités du fait du manque d'effectivité des mesures prises par certaines d'entre elles[85], pourtant chefs de file, tantôt par d'autres ou les mêmes qui réclament au nom de l'effet utile une certaine compétence[86]. Au-delà, la

85. À cet égard, voir les griefs en particulier adressés par l'APD allemande vis-à-vis de l'APD irlandaise et les faiblesses de l'APD luxembourgeoise, développés par R. Perray, « Trois ans après l'entrée en vigueur du RGPD : quel est le bilan de la coopération administrative entre les autorités de protection des données à caractère personnel », dossier : « RGPD, Cinq ans après », *Rev. aff. eur.* 2021, n° 1, p. 50 et 51.

86. V. à ce sujet, l'affaire *Facebook Ireland Ltd and Facebook Belgium Ltd c/ APD belge*. CJUE 15 juin 2021, aff. C-645/19 où la Cour de Luxembourg a finalement décidé : « L'article 55, paragraphe 1, et les articles 56 à 58 ainsi que 60 à 66 du 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), lus en combinaison avec les articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne, doivent être interprétés en ce sens qu'une autorité de contrôle d'un État membre qui, en vertu de la législation nationale adoptée en exécution de l'article 58, paragraphe 5, de ce règlement, a le pouvoir de porter toute prétendue violation dudit règlement à l'attention d'une juridiction de cet État membre et, le cas échéant, d'ester en justice peut exercer ce pouvoir en ce qui concerne un traitement de données transfrontalier, alors qu'elle n'est pas l'"autorité de contrôle chef de file", au sens de l'article 56, paragraphe 1, du même règlement, s'agissant de ce traitement de données, pour autant que ce soit dans l'une des situations où le règlement 2016/679 confère à

transformation du Groupe de l'article 29 en un Comité européen de protection des données (en abrégé CEPD) limite l'autonomie des différentes autorités nationales de protection des données.

On note que le CEPD (articles 68 s.) dispose de pas moins de 25 chefs de compétence suivant l'article 70.1. Il peut intervenir en cas de conflit entre une autorité chef de file et celles concernées (article 65.1). Là où la directive parlait d'avis ou opinions, l'article lui confie le soin d'élaborer des « lignes directrices », des « recommandations » ou des « bonnes pratiques ». Leur multiplication[87] dans tous les domaines fait qu'elles constituent une réelle source secondaire de la réglementation européenne de protection des données. Enfin, l'article 64.1 du RGPD oblige les APD nationales à soumettre au CEPD leurs projets de décisions sur 6 points en tout cas (par exemple : les projets de code de conduite ; les clauses contractuelles type en cas de flux transfrontières ; les projets d'agrément des organismes de certification, etc.). Il n'y a pas loin, nonobstant la résistance de certaines APD nationales, de considérer comme envisageable à moyen terme, la création d'une seule APD européenne, certes avec des décentralisations nationales. Et l'exemple du CEPD comme outil de pleine cohérence de l'exécution d'une politique européenne et ne laissant qu'une marge de manœuvre très subsidiaire aux États membres et à leurs organes semble inspirer d'autres domaines d'action de l'Union européenne.

26. Cette mise en exergue d'une législation pleinement cohérente est par ailleurs bien utile au moment où l'Union européenne entend faire de son modèle « Protection des données » le pilier de sa « troisième voie » relative au développement du numérique[88]. Sans être long, disons qu'il s'agit pour l'UE de devenir face à ses adversaires tant chinois qu'américains[89] les champions

cette autorité de contrôle une compétence pour adopter une décision constatant que ledit traitement méconnaît les règles qu'il contient ainsi que dans le respect des procédures de coopération et de contrôle de la cohérence prévues par ce règlement. »

87. On dénombre 29 lignes directrices et recommandations depuis la création de la CEPD, sans compter la reprise de toute une série d'avis et d'opinions émises par le Groupe de l'article 29 d'ancien régime. Outre une interprétation quasi systématique des concepts utilisés par le RGPD, on note des documents donnant suite à des décisions de la CJUE (par exemple, dans le cas des affaires *Schrems I et II*), d'autres relatives à des thématiques comme le *profiling* ou à des technologies, comme l'IA ou les assistants virtuels vocaux, etc. ; d'autres, enfin, sur des mécanismes mis en place par le RGPD (ex. : les *Security Breaches* ; les *Privacy by design* ou les *Privacy Impact Assessments*).

88. Sur la dimension politique du débat de la protection des données, lire les réflexions de H. Burkert, « The European Data Protection and information Governance », *in* J. Herveg (dir.), *Deep Diving into Data Protection*, Cahier du CRIDS, 2021, n° 51, en particulier, p. 16 s.

89. L'option européenne constitue une stratégie explicitement énoncée et progressivement mise en œuvre à travers des textes qui se suivent à un rythme accéléré. Elle peut se résumer comme suit : *« The global leadership of Europe in adopting the latest technologies, seizing the benefits and promoting the development of human-centric, sustainable, secure, inclusive and trustworthy artificial intelligence (AI) depends on the ability of the European Union (EU) to accelerate, act and align AI policy priorities and investments. This is the key message and a*

d'une politique du numérique fondée sur « l'excellence et la confiance » et ainsi s'assurer d'un leadership mondial en la matière. La volonté exprimée à de nombreuses reprises par les autorités européennes est en effet de fonder le développement des outils et des applications d'intelligence artificielle sur deux valeurs : *« Excellence and Trust »*, selon le titre même du Livre blanc sur l'IA *(White Paper on AI)* de février 2020[90], document à la base de cette politique qui marque la troisième voie européenne. La protection des données à caractère personnel est d'emblée identifiée par les stratèges européens comme la pièce centrale qui permet d'inspirer la confiance des citoyens. Dès son investiture, soit en novembre 2019, Ursula von der Leyen, présidente de la Commission européenne, lors de son allocution devant le Parlement, affirmait : « We must have mastery and ownership of key technologies in Europe. These include quantum computing, artificial intelligence, blockchain, and critical chip technologies [...] *With the General Data Protection Regulation*, we set the pattern for the world. We have to do the same with artificial intelligence. Because in Europe we start with the human being. It is not about damming up the flow of data. » Nous reviendrons sur ce point en conclusion (*infra*, n° 31).

27. Revenons aux dispositions relatives aux flux transfrontières. La dimension internationale des flux est présente dès 1980 et s'illustre à travers les textes fondateurs des organisations internationales, qu'il s'agisse des Nations unies[91],

vision of this 2021 review of the Coordinated Plan. » Il s'agit bien d'une troisième voie dans la mesure où l'Union européenne entend mener une politique de développement de l'IA fondée sur des principes différents de ceux qui fondent, d'une part, la politique américaine que, sans doute à tort, on résumera par un « tout au marché » et, plus justement, par la volonté de maintenir et de développer le leadership américain et, d'autre part, la politique chinoise marquée par un interventionnisme de l'État et une IA au service de l'économie, de la gouvernance sociale par l'État et de la sécurité de ce dernier.

90. *White Paper on Artificial Intelligence. A European approach to excellence and trust*, Brussels, 19 févr. 2020 COM(2020) 65 final. En matière d'excellence, selon le résumé de la Commission elle-même, le « Livre blanc » propose les mesures suivantes : « 1. Mettre en place un nouveau partenariat public-privé dans les domaines de l'IA et de la robotique ; 2. Renforcer les centres d'excellence en matière d'IA et les relier ; 3. Faire en sorte qu'au moins un pôle d'innovation numérique par État membre soit spécialisé en IA ; 4. Fournir davantage de financement au développement et à l'utilisation de l'IA, avec le soutien du Fonds européen d'investissement ; 5. Utiliser l'IA pour améliorer l'efficacité des procédures de marchés publics ; 6. Soutenir l'acquisition de systèmes d'IA par des organismes publics. » En matière de confiance, la Commission propose de : « 1. Veiller à ce que la nouvelle législation sur l'IA tienne compte des risques mais n'entrave pas l'innovation ; 2. Exiger que les systèmes d'IA à haut risque soient transparents, traçables et sous contrôle humain ; 3. Donner aux autorités les moyens de vérifier la conformité des systèmes d'IA, tout comme elles le font avec les cosmétiques, les voitures ou les jouets ; 4. Veiller à ce que les ensembles de données ne soient pas entachés de biais ; 5. Lancer un débat à l'échelle de l'UE sur l'utilisation de l'identification via les technologies de la reconnaissance faciale. »

91. Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, adoptée le 14 déc. 1990 par l'Assemblée générale des Nations unies dans sa résolution 45/95 du 14 déc. 1990.

de l'OCDE[92] ou du Conseil de l'Europe. L'article 9 de la résolution onusienne[93] traduit bien le relatif laxisme des premières réglementations : « Lorsque la législation de deux ou plusieurs pays, concernés par un flux transfrontière de données, présente des garanties comparables au regard de la protection de la vie privée, les informations doivent pouvoir circuler aussi librement qu'à l'intérieur de chacun des territoires concernés. En l'absence de garanties comparables, des limitations à cette circulation ne peuvent être imposées indûment et seulement dans la stricte mesure où la protection de la vie privée l'exige. » La directive de 1995 devait adopter un standard plus élevé, il s'agissait d'assurer une protection européenne de haut niveau aux citoyens européens. Les articles 25 et suivants réclament une protection adéquate. Cette notion de protection adéquate a fait couler beaucoup d'encre. Elle se distingue tant de celui de protection suffisante que de celui de protection équivalente. Elle est entendue comme une protection permettant, peu importent les moyens, d'assurer effectivement les principes mêmes de la directive et les prérogatives de la personne concernée. Il ne s'agit donc pas de réclamer une identité de contenu mais bien celle d'une effectivité de la protection des personnes concernées par des méthodes qui peuvent être originales et relever principalement de l'autorégulation. Cette protection peut exister au niveau d'un pays, à la limite à un niveau sectoriel, mais peut également être réalisée par un contrat ou se déduire des caractéristiques du flux en question. Par ailleurs, on ajoute que la directive (article 4) s'applique dès qu'un traitement même situé hors Union européenne peut s'appuyer sur des moyens localisés, eux, sur le territoire de l'Union.

En matière de flux transfrontières, les articles 44 et suivants du règlement reprennent l'essentiel du système proposé par les articles 25 et suivants de la directive même si la formulation est plus positive. Le règlement abandonne en effet l'interdiction de principe au profit d'une formulation plus positive : « Un transfert de données à caractère personnel vers un pays tiers ou une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision[94] que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. » Ceci dit, l'évaluation du caractère adéquat renvoie désormais à des critères plus nombreux et donc plus exigeants. En particulier, il est « tenu compte » de l'existence d'une

92. Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptée par le conseil des ministres de l'OCDE le 23 sept. 1980 (amendée le 11 juill. 2013).

93. L'article 12 de la convention n° 108 énonce qu'entre parties contractantes c'est-à-dire ayant un instrument législatif reprenant les principes de la convention, le principe est la non-interdiction de flux transfrontières sauf deux exceptions : l'existence de législations spécialisées et l'utilisation d'un pays signataire comme simple transit vers un pays non signataire, afin de contourner la protection offerte par l'État d'origine.

94. Notons que ces décisions de la Commission peuvent faire l'objet de recours par toute personne concernée devant la Cour de justice selon l'article 263 du TFUE.

autorité de contrôle indépendante disposant de pouvoirs d'action effectifs et des engagements internationaux, en ce compris la participation à des systèmes multilatéraux (comme la référence aux principes directeurs de l'OCDE ou la signature de la convention dite n° 181 du Conseil de l'Europe sur la vie privée et des engagements régionaux de protection des données comme l'*APEC Privacy Framework* adopté dans le cadre de l'accord de coopération économique entre pays du Sud-Est Asie-Pacifique[95]).

On souligne en outre que ces critères débordent la régulation du secteur privé pour couvrir également celle du secteur public, en particulier les possibilités pour les autorités publiques d'exiger du secteur privé la communication des données obtenues. Ainsi, à la suite de l'arrêt *Schrems I*[96], « il est tenu compte de la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation ». On ajoute que cet arrêt abandonne la signification pragmatique donnée au terme « adéquate » pour une exigence plus forte, celle de « substantiellement équivalente[97] ». L'adéquation de la protection peut se réaliser par des techniques dont le nombre a été élargi aux codes de conduite et aux règles d'entreprise contraignantes, sachant que peu importe

95. Sur cet accord, lire : [https://www.apec.org/publications?pub_id=390]. Pour une comparaison entre l'APEC Privacy Framework et le règlement européen, lire l'article publié sur le site de l'IAPP : [https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/].

96. L'arrêt *Schrems* (CJCE 6 oct. 2015, aff. 362/14), dans une affaire concernant Facebook, considère en effet que le niveau de protection offert par les États-Unis n'est pas satisfaisant, nonobstant la décision d'adéquation de la Commission européenne dite *« Safe Harbor »* du 26 juill. 2000, dans la mesure où cette décision ne prend pas en compte les risques de violation de la vie privée suite aux activités de la National Security Agency des États-Unis. Comme on le sait, cet arrêt a obligé les États-Unis et la Commission européenne à conclure un nouvel accord : les *« Privacy Shields »*.

97. « Cette juridiction souligne que, dans l'arrêt *Schrems*, la Cour a interprété l'article 25, paragraphe 6, de la directive 95/46 (dont le contenu est essentiellement repris à l'article 45, paragraphe 3, du RGPD), en ce qu'il prévoyait que la Commission ne peut adopter une décision d'adéquation qu'après s'être assurée que le pays tiers visé garantit un niveau de protection adéquat, comme supposant que celle-ci établisse que ce pays assure un niveau de protection des libertés et droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de cette directive, lue à la lumière de la Charte » (arrêt *Schrems II* [CJUE 16 juill. 2020, aff. C-311/18]) confirmant les attendus de l'arrêt *Schrems* I (§ 73) : « Certes, le terme "adéquat" figurant à l'article 25, paragraphe 6, de la directive 95/46 implique qu'il ne saurait être exigé qu'un pays tiers assure un niveau de protection identique à celui garanti dans l'ordre juridique de l'Union. Toutefois, comme l'a relevé M. l'avocat général au point 141 de ses conclusions, l'expression "niveau de protection adéquat" doit être comprise comme exigeant que ce pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive 95/46, lue à la lumière de la Charte. »

la technique choisie, les exigences doivent être les mêmes, précise l'arrêt *Schrems II*[98].

28. L'article 3 du RGPD précise le champ d'application « territorial » du règlement. Le critère principal est celui du public visé par l'établissement qui opère le traitement[99] et non la localisation de celui-ci : « Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union. » On ne peut que se féliciter de ce choix dans la mesure où les technologies, en particulier celles du *cloud computing*, permettent de localiser où on le souhaite la matérialité du traitement. Cette *extension extra-territoriale* (entendre hors Union européenne) des effets du règlement[100] est remarquable. On se souvient que l'article 4 alinéa 1er de la directive 95/46 avait déjà fait preuve d'audace en appliquant les prescrits européens à des traitements hors Union européenne opérés par des établissements situés en dehors de l'Europe lorsque ces traitements concernaient des personnes situées sur le territoire de l'Union et *« faisaient usage »* d'équipements situés en Europe, par exemple, lorsque les données étaient recueillies via des cookies ou autres serveurs situés en Europe. Avec le nouveau texte, les prescrits européens s'appliqueront désormais à des traitements même situés hors Europe par des établissements non européens si leur cible consiste en une clientèle européenne qu'il s'agisse, soit de leur offrir même gratuitement des biens et

98. « Les articles 45 et 46 du RGPD ont pour but d'assurer la continuité du niveau élevé de protection des données à caractère personnel assuré par ce règlement lorsqu'elles sont transférées en dehors de l'Union. En effet, l'article 44 du RGPD, intitulé "Principe général applicable aux transferts", ouvre le chapitre V relatif aux transferts vers des pays tiers en énonçant que toutes les dispositions de ce chapitre sont appliquées de manière à ce que le niveau de protection garanti par le RGPD ne soit pas compromis en cas de transfert vers un État tiers. Cette règle vise à éviter que les standards de protection découlant du droit de l'Union soient contournés en transférant des données à caractère personnel vers un pays tiers en vue de les y traiter. Au regard de cet objectif, il est indifférent que le transfert soit fondé sur une décision d'adéquation ou sur des garanties offertes par le responsable du traitement, notamment au moyen de clauses contractuelles. Les exigences de protection des droits fondamentaux garantis par la Charte ne connaissent pas de distinction en fonction du fondement légal sur lequel repose un transfert déterminé » (arrêt *Schrems II*, cité note précédente, § 117). Cet arrêt a été rendu à propos de clauses contractuelles signées par Facebook et suscite de nombreuses questions sur l'évaluation de ce caractère « substantiellement équivalent » en dehors des décisions d'adéquation.

99. Dans l'affaire Google, la Cour de justice de Strasbourg avait de même estimé que les services de moteurs de recherche rendus par Google devaient être soumis aux dispositions de la directive applicables aux responsables de traitement européens au motif que ces services utilisaient, du moins pour le public espagnol, les ressources publicitaires d'une succursale de Google située en Espagne.

100. ... sous réserve de ce que nous dirons à propos des flux transfrontières entre un responsable sis en Union européenne ou visé par le champ d'application territorial du règlement et un responsable non couvert par ce champ d'application.

services, soit de suivre leur comportement au sein de l'Union (exemple : pour Google, récolter via Androïd les données de localisation de smartphones).

On s'interroge sur ce qui peut être interprété comme un « impérialisme » de la protection européenne des données face au reste du monde. Cette rhétorique poussée dans le dos par une Cour de justice assertive et construite sur un imperium européen a-t-elle les moyens de son ambition et les dispositions imposées unilatéralement par notre RGPD n'appellent-elles pas des réponses unilatérales d'autres puissances bien plus armées pour les imposer que nous, s'interroge avec raison M^me^ Benabou[101]. Témoigne de ce risque, l'*US Cloud Act*. Les dispositions unilatérales imposées aux opérateurs américains par ce texte[102] ont des conséquences sur les utilisations faites par les entreprises européennes des services de ces opérateurs et donc peuvent concerner des données à caractère personnel. Le pari européen de la protection des données à caractère personnel est courageux et à féliciter mais est-il réaliste ? Le temps nous le dira.

CONCLUSIONS

29. Que tirer de cette histoire de 50 ans de législations européennes de protection des données ? L'article 8, conçu dans une civilisation sans ordinateur mais progressivement conçu comme droit à l'autodétermination, a rapidement donné naissance dès 1970 à des législations qui, prenant conscience du pouvoir que donnait l'information à l'autorité publique et à certaines entreprises privées, nécessitaient des législations capables de limiter ce pouvoir informationnel. Au-delà des premières esquisses que représentaient les résolutions de 1973 et de 1974, le Conseil de l'Europe de 1981 a compris qu'il était important, obligation positive des États, de dériver des exigences du droit à la vie privée ou à l'autodétermination, un droit à la protection des données qu'affirme désormais la convention n° 108. Il s'agit d'assurer notre « auto-détermination informationnelle », comme le reconnait explicitement, dès 1983, la Cour constitutionnelle allemande. Au

101. V.-L. Benabou, « Le RGPD ou la ligne Maginot de la protection des données personnelles face aux acteurs européens », *in* dossier : « RGPD, Cinq ans après », *Rev. aff. eur.* 2021, n° 1, p. 61 s. L'auteure souligne ainsi les dangers de la réponse américaine que constitue le *Cloud Act*.

102. Soit le *Clarifying Lawful Overseas Use of Data Act*, adopté le 23 mars 2018 (*Pub-Law.* 115-141). Cette approche unilatérale risquant de mettre à mal la protection des données européenes est dénoncée par l'EDPB et l'EDPS (*Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence*, 10 juill. 2019) : *« By choosing to create a legal avenue under US law for US law enforcement authorities to require disclosure of personal data directly from service providers who fall under US jurisdiction, irrespective of where the data is stored, the US Congress enacts into US law a practice of US governmental entities likely to bypass the Mutual legal assistance in criminal matters treaty (MLAT)2 in force between the European Union and the United States of America. »*

niveau de l'Union européenne, si ce sont bien les impératifs du commerce et les exigences d'assurer une libre circulation des données à caractère personnel qui fondent la directive de l'Union européenne de 1995 et expliquent la marge de manœuvre – certes réduite mais réelle – laissée aux États membres, la reconnaissance d'un droit quasi constitutionnel par la Charte et l'élargissement des compétences de l'Europe aux droits de l'homme ont légitimé cette fois une politique plus proactive de l'Union européenne, qui devait déboucher sur le RGPD et une protection harmonisée même si çà et là quelques failles se font jour.

Au-delà de ce rappel historique, nous nous risquons à certaines réflexions. La première note que ces législations, loin d'être inscrites dans le marbre, suivent les évolutions technologiques et rendent nécessaires leur évaluation continue et, par voie de conséquence, leur évolution[103]. Ainsi, l'irruption ubiquitaire de l'Internet, la multiplication des acteurs, les capacités à l'infini de traitement de nos ordinateurs ont bouleversé, et sans doute encore insuffisamment, les concepts de base de nos législations. Au-delà, faut-il voir, ne serait-ce qu'avec l'allongement des textes[104], une préoccupation du législateur de ne plus se contenter de principes mais d'exiger par la multiplication d'obligations pour les acteurs, par la multiplication des droits subjectifs octroyés, par les mesures procédurales observées, par le renforcement des compétences des autorités de protection des données et l'attention à une technique *« compliant »*, une volonté d'effectivité maximale du texte législatif désormais unique. À ces longueur et complexité du RGPD, s'ajoute, faut-il le souligner, son interprétation hardie à la fois par l'*European Data Protection Board* ou l'*European Data Protection Supervisor*, d'une part, et par la CJUE, d'autre part.

30. Le renforcement du texte à la fois tant dans son contenu que dans son effectivité y compris en dehors des frontières explique que la protection des données jouit d'un statut particulier parmi l'ensemble des libertés et droits individuels. Si on songe à la liberté d'expression voire au droit de la consommation, il est clair que celle-ci ne dispose pas d'un arsenal législatif et administratif de protection aussi impressionnant et aussi structuré. On ne s'étonne pas dès lors que la protection des données soit un pilier de la stratégie européenne, en matière de politique du numérique dite de la « 3^e^ voie[105] ».

103. Plus que la technologie en constante évolution c'est l'impact et les enjeux de l'utilisation de ces technologies qui rendent nécessaires l'évolution technologique.

104. La convention n° 108 contenait 17 articles ; la directive, pas moins de 34 articles ; le RGPD, 99 sans compter les innombrables avis et opinions de l'EDPB et de l'EDPS indispensables pour connaître l'interprétation à donner au texte de l'Union européenne.

105. Lire à cet égard, nos réflexions sur cette troisième voie européenne, « "La troisième voie" une voie difficile. Quelques réflexions autour de la politique européenne en matière d'intelligence artificielle », *RLDI*, juin 2021, n° 182, p. 32 s.

Tout est-il rose pour autant au pays de la protection des données ? Notre propos, tout en reconnaissant les mérites de l'action européenne, s'interroge sur la dimension politique qu'incontestablement a pris la réglementation de protection des données dans le cadre des dispositions du RGPD sur les flux transfrontières mais également dans la recherche d'une application uniforme de la réglementation et dans une politique de certificats européens, qui permette d'asseoir sa souveraineté. L'Europe est-elle en mesure de gagner son pari souverain voire « impérialiste » ? La protection des données est ainsi mise au service de cette politique européenne de la troisième voie du développement du numérique et on sent dès lors les autorités européennes arcboutées sur un texte, au risque de ne pas se donner la liberté de le faire évoluer, ce qui nous semble pourtant nécessaire. Par ailleurs, pour rester sur le registre « politique », l'Europe peut-elle imposer son modèle de protection des données à la terre entière voire à l'Europe entière[106] au détriment de la saine émulation qui pouvait exister entre interprétations nationales[107].

Par ailleurs, la réglementation, conçue avec les premiers textes du RGPD il y a près de 10 ans maintenant, souffre déjà de sa confrontation avec les développements récents du numérique. L'irruption des technologies comme la *blockchain* ou l'intelligence artificielle rend difficile l'exercice des droits subjectifs de la personne concernée et met à mal les principes de base du bon responsable de traitement. La multiplication des opérations de partage des données entre responsables de traitement, la capacité dorénavant sans limite des traitements de données obligent à des interprétations de plus en plus hardies des concepts même de la réglementation. S'il ne peut être question de multiplier des législations *ad hoc* pour ces différentes technologies, on pressent qu'il sera nécessaire de lancer de nouveaux débats publics sur l'acceptabilité sociétale de ces nouvelles technologies.

31. On ajoute que les législations européennes ont évolué dans une direction contestable, en s'orientant vers une conception de plus en plus individualiste de la protection des données. La consécration du consentement comme première cause de légitimité, la multiplication des droits subjectifs confèrent à l'individu une responsabilité de plus en plus grande dans la protection de « ses » données. Ce dernier en est-il capable à l'heure de l'ubiquité et de l'opacité des traitements ? La dimension individualiste est-elle la bonne optique à

106. Comme en témoigne la récente résolution du Parlement européen ayant mis en demeure l'Irlande de veiller au respect du RGPD, suite à l'affaire *Schrems II*. V. la résolution du Parlement européen du 20 mai 2021 sur l'arrêt rendu par la Cour de justice de l'Union européenne le 16 juill. 2020 dans l'affaire C-311/18, *Data Protection Commissioner c/ Facebook Ireland Ltd et Maximillian Schrems* (« arrêt *Schrems II* ») (2020/2789[RSP]) disponible à l'adresse : [https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_FR.pdf].

107. À cet égard, si on note le succès certes croissant des pays signataires de la convention n° 108 + du Conseil de l'Europe, ne sont-ce pas les marges de manœuvre importantes laissées aux États signataires qui justifient ce succès ?

l'heure où les discussions sur l'éthique en particulier de l'intelligence artificielle soulignent les enjeux collectifs voire sociétaux des traitements de données. La prise en considération de tels enjeux obligerait les autorités de protection des données, si, comme elles le réclament, elles veulent être les futures autorités compétentes de l'évaluation des applications de cette technologie, à élargir leur point de vue, la capacité de saisine par des associations et à s'ouvrir à d'autres dimensions, celles de justice sociale, de démocratie, de protection de l'environnement, etc. Ne faut-il pas également les doter de moyens pour pouvoir sensibiliser, informer davantage le public, susciter le débat public, créer des outils, guichets d'information, etc. ? Ce n'est peut-être pas leur rôle aujourd'hui mais n'y aurait-il pas à lancer une réflexion sur le sujet, en parallèle avec les développements législatifs ? N'est-il pas important dans cette optique de refonder l'action de ces autorités et celle législative sur le concept de vie privée, au sens qui lui est donné par la Cour de Strasbourg ?

Enfin, ne faut-il pas, comme le RGPD l'a initié, mais comme l'ont bien compris les rédacteurs des textes législatifs relatifs à l'intelligence artificielle, se centrer sur les risques tant individuels, collectifs, que sociétaires des innovations du numérique et instituer des procédures internes et externes ouvertes de gestion et d'évaluation des risques et cela de manière plus encadrée que la procédure de *Privacy Impact Assessment* prévue de manière très limitée par le RGPD[108]. Cette focalisation devrait amener à ne pas exiger de tous les responsables de traitement les mêmes exigences comme le réclame le RGPD[109]. Il s'agit, plutôt que d'insister en vain sur la responsabilité des personnes concernées via la reconnaissance de l'importance de leur consentement et de la multiplication de droits subjectifs à leur bénéfice, de souligner la responsabilité sociétale de tous les acteurs qui participent activement à la numérisation de la société et de les obliger à mettre en place des procédures d'évaluation des risques créés et des voies y compris technologiques de leur maîtrise[110]. Il

108. La liste, reprise en annexe du projet de règlement : *Artificial Intelligence Act*, des applications de l'IA dites à haut risque pose question : c'est en priorité au regard des enjeux de protection des données que la plupart de ces applications y figurent. Comment dès lors vont se concilier les procédures mises en place par la proposition de règlement européen à propos de l'IA et les exigences du RGPD ? Qui y procédera ?, et comment résoudre les conflits de décision en cas de pluralités d'organes compétents ?

109. Deux nuances à ce propos : premièrement relevons qu'à juste titre, dans l'*Artificial Intelligence Act* proposé par la Commission, c'est essentiellement l'examen de la finalité des applications qui détermine la hauteur du risque ; secondement, le RGPD, s'il soumet en principe tous les traitements à même réglementation, prévoit cependant des exceptions, liées à la nature des données (voir les traitements de données sensibles) ou à la finalité (voir en particulier les traitements conduisant à des décisions automatisées). Par ailleurs, la nomination d'un DPO ou l'évaluation des risques (PIA) ne sont pas imposées à tout responsable ou à tout traitement.

110. C'est le « *shift* » auquel invite un auteur comme V. Mayer-Schönberger (« Paradigme Shift », *CLS&R* 2021, n° 40, 105515), « *The focus ought not to be informed consent, which in practice equates to individual responsibility... Responsibility needs to rest with those that have a better capacity to understand, foresee and act. Evolving data protection by shifting far more*

s'agit, au-delà, de créer des organismes publics participatifs et inclusifs de « *Technology Assessment*[111] » afin d'instiller au cœur de la technologie et de la gestion responsable de ses applications, les garanties nécessaires à la survie de nos libertés tant individuelles que collectives et de nos démocraties, n'est-ce pas ce à quoi nous invitent 50 ans de législations de protection des données ?

responsibility to data processors and users is not a crazy novel idea... It was the fundamental principle of the first data protection laws... » V. aussi dans le même sens les écrits de H. Burkert et de B. van der Sloot déjà cités.

111. Sur ce point, nos réflexions *in* Y. Poullet, *Éthique et droits de l'homme dans notre société du numérique*, Mémoire de l'Académie royale de Belgique, 2020, p. 157 s.