Cinq ans après – le RGPD est-il toujours la solution ?

Poullet, Yves

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2023

Document Version
le PDF de l'éditeur

DOCTRINE

Cinq ans après – le RGPD est-il toujours la solution ?

Yves Poullet[1]

Is the GDPR offering an adequate solution to protect our liberties in an evolving digital society ? The answer is definitively not as positive as some GDPR supporters claim without nuance, for different reasons. First, the excessive complexity of this legal framework must be underlined. In addition, we are of opinion that more and more data protection authorities are perceived as judges and controllers rather than facilitators. Second, the broad legislative scope of the GDPR and its extraterritorial effect put our regulators at risks of a certain imperialism and of hindering technological innovation. Third, it is necessary to attentively analyze the adequacy of the GDPR concepts in relation to emerging technologies (AI, IoT and NBIC applications), and to their ecosystems. Fourth, questions arise as regards the concepts of personal and sensitive data, as well as regarding the potential need to add new categories of actors to be regulated by the GDPR. These questions emerge due to a context of new actors entering supply chains, and of activities and services being delivered by platforms and shared infrastructures. Finally, this paper invites the reader to put into question the individualistic approach of the GDPR, which is based on the exercise of individual rights, at a time where collective challenges to the social justice and democracy are more and more at stake.

• • •

Le RGPD offre-t-il une solution adéquate pour protéger nos libertés, dans une société numérique en constante évolution ? Pour différentes raisons, la réponse à cette question n'est définitivement pas aussi positive que celle proclamée, sans nuance, par les partisans du RGPD. Premièrement, la complexité excessive de cette législation doit être soulignée. De plus, selon nous, les autorités de protection des données sont de plus en plus perçues comme des juges et des contrôleurs, plutôt que comme des facilitateurs. Deuxièmement, le large champ d'application du RGPD et son effet extraterritorial font courir les risques d'un certain impérialisme, et d'entraver l'innovation technologique. Troisièmement, il est nécessaire d'analyser attentivement l'adéquation des concepts du RGPD face aux technologies émergentes et à leurs écosystèmes, qu'il s'agisse de l'IA, de l'IoT ou des applications NBIC. Quatrièmement, nous nous interrogeons quant aux concepts de données à caractère personnel et de données à caractère personnel dites « sensibles », et sur la nécessité d'ajouter de nouvelles catégories d'acteurs à réguler par le RGPD. Ces questions émergent d'un contexte dans lequel de nouveaux acteurs entrent dans les chaînes d'approvisionnement, et dans lequel des activités et des services sont délivrés par des

[1] Professeur émérite de l'Université de Namur, membre de la chambre juridictionnelle de l'APD belge et de la Commission de contrôle des fichiers (CCF) d'Interpol, membre de l'Académie royale de Belgique. L'auteur tient tout particulièrement à remercier M^me^ M. Knockaert, chercheuse senior au CRIDS/NaDI, pour sa lecture patiente de cette contribution, en particulier pour ses heureuses suggestions.

plateformes et des infrastructures partagées. Enfin, cet article invite le lecteur à remettre en question l'approche individualiste du RGPD, fondée sur l'exercice de droits individuels, à l'heure où les enjeux collectifs de justice sociale et de démocratie sont de plus en plus présents.

1. Qui aime bien châtie bien… chacun connaît mes convictions affirmées et ma passion en faveur de la défense de la vie privée, à défaut en faveur de la protection des données. Que mes dires aujourd'hui ne soient pas interprétés comme le reniement de ces positions mais plutôt comme l'expression de certains doutes à propos de ce que je crois être un dogmatisme de la protection des données, dogmatisme autour d'une sainte Bible : le RGPD[2].

Mon propos s'articulera en cinq points.

Le premier (I) s'adresse à la complexité et à la démesure de cette législation. Le deuxième (II), à l'ampleur de son domaine d'application. En particulier, il s'inquiète des visées géopolitiques européennes qui à la fois confèrent à ce texte une valeur symbolique de représentation des valeurs européennes au risque d'un certain impérialisme mais, dans le même temps, le rendent fragile au regard des préoccupations plus économiques qui sont celles de l'Europe. Comment concilier protection des données et développement de l'innovation ? Le troisième (III) analyse l'adéquation du RGPD à l'heure et face à la réalité des technologies émergentes et des écosystèmes mis en place, qu'il s'agisse de l'intelligence artificielle (« IA »), de l'internet des objets (« IoT ») ou des applications des NBIC. Le quatrième (IV) interroge le concept de données à caractère personnel, s'inquiète de l'insuffisance des acteurs réglementés par le RGPD, à l'heure des plateformes et des infrastructures partagées Enfin, le cinquième (V) pointe la lacune fondamentale de l'approche individualiste qui sous-tend la réglementation sur la protection des données et, en particulier, remet en cause la prédominance du consentement comme cause de licéité des traitements.

Chacun de ces points appelle les réflexions suivantes.

I. LA MULTIPLICATION ET LA COMPLEXITÉ DES TEXTES ET DES PROCÉDURES

2. Les textes sur la protection des données sont légion. À un RGPD, qui compte 99 articles, là où la Convention 108+[3] se contente de 30 dispositions, s'ajoute la directive (UE) 2016/680, directive « Police »[4], à la longueur et au contenu tout aussi prolifiques. Le praticien de la protection des données ne peut se passer d'une analyse des nombreuses opinions,

[2] 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, *J.O.*, L 119, 4 mai 2016.

[3] Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), signé à Elseneur, 18 mai 2018.

[4] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.*, L 119/89, 4 mai 2016.

recommandations, lignes de conduite émanant des instances du Comité européen de la protection des données (« CEPD ») et du CEPS[5], émises non sans raison certes mais dont la lecture s'avère épuisante, jamais achevée et adoptant un vocabulaire ésotérique. À cela, s'ajoute une jurisprudence émanant à la fois des autorités de protection des données (« APD ») nationales et parfois régionales[6] mais surtout de la Cour de justice de Luxembourg de plus en plus sollicitée[7] et dont l'interprétation des textes est souvent innovante et hardie. Que l'on songe à titre de simples exemples, aux arrêts *Schrems*[8] ou aux récents arrêts en matière de rétention des données ou de PNR[9].

C'est à travers ce labyrinthe de textes que le praticien de la protection des données se doit de naviguer. La matière des droits de l'homme eût sans doute exigé pour en permettre l'accès à tous, l'énoncé de seuls quelques principes, laissant aux juridictions le soin d'interprétations parfois divergentes mais dont la cohérence pouvait s'obtenir à travers le temps et l'existence d'une APD européenne. Derrière cette première critique s'en cache une plus fondamentale, le fait que la protection des données devient une matière réservée à des cabinets de praticiens aux épaules solides et pas toujours, loin s'en faut, européens.

3. À cette complexité des textes s'ajoutent celles des institutions et des procédures. Chaque pays dispose en fonction de ses propres traditions et de ses propres choix d'une autorité dont l'indépendance, la composition et le fonctionnement interne peuvent se concevoir différemment. La saisine en cas de litige se décline différemment et suit des règles tantôt proches de celles d'une instance judiciaire, tantôt plus conçues sous le mode administratif où le plaignant joue un rôle à la seule introduction du litige[10]. Les décisions se lisent de manière différente et les recours impliquent des juridictions d'appel de nature très différente. On ajoute que la dimension européenne de la plupart des traitements en cause ne facilite pas la vie ni des plaignants à la recherche de la bonne porte d'entrée, ni des autorités qui s'interrogent sur le critère à suivre en ce qui concerne la désignation de l'autorité chef de file, sans compter la nécessité de

5 Selon le site internet Wikipedia : « En 2009, par exemple, le CEPD a adopté plus de cent avis de contrôle préalable, portant essentiellement sur des questions telles que les données médicales, l'évaluation du personnel, le recrutement, la gestion du temps de travail, les outils d'enregistrement téléphonique et les enquêtes de sécurité » (Wikipedia, *v°* « CEPD »). En 2021, le rapport annuel du CEPD recense pas moins de 17 avis au titre de l'article 42 et d'avis conjoints du CEPD et du Comité européen de la protection des données émis en réponse aux demandes de consultation législative de la Commission européenne. Ce rapport est disponible à l'adresse suivante : https://edps.europa.eu/annual-reports_fr.

6 Tel est le cas en Allemagne et en Belgique même si récemment la Cour constitutionnelle a clairement établi la prééminence de l'APD fédérale sur les organes de protection des données créées dans les entités fédérées ; C. const., 16 février 2023, n° 26/2023.

7 Info-Curia renseigne plus de 100 affaires en matière de protection des données depuis 2017. La consultation du site témoigne d'une augmentation importante du nombre de recours ces trois dernières années.

8 C.J., 6 octobre 2015, arrêt *Maximilian Schrems c. Data Protection Commissioner*, C-362/14 ; C.J., 16 juillet 2020, arrêt *Data Protection Commissionner c. Facebook Ireland Ltd et Maximilian Schrems*, C-311/18.

9 C.J., 21 juin 2022, arrêt *Ligue des droits humains c. Conseil des ministres*, C-817/19. Dans cet arrêt, la Cour de justice de l'Union européenne se montre rétive à l'utilisation d'outils d'intelligence artificielle de *machine learning* pour détecter des passagers terroristes, dans la mesure où le fonctionnement de ces outils permet l'évolution des critères de suspicion et que l'opacité de tels traitements interdit le recours utile des personnes suspectées.

10 Ainsi, en France, dès réception d'une plainte, la CNIL se charge de l'instruction du dossier alors qu'en Belgique, la procédure est menée, sauf exceptions (saisine directe par l'APD), par le plaignant et l'APD est restreinte à l'objet de la plainte, comme le lui a rappelé à plusieurs reprises la Cour des marchés.

concertation entre les autorités des pays impliqués par le traitement (la procédure dite IMI).

Ne peut-on imaginer la création d'une autorité européenne de protection des données, compétente pour tout litige ayant une dimension européenne ou affectant un nombre substantiel d'États membres ? Les autorités nationales renverraient systématiquement les causes ayant une telle dimension à cette autorité où seraient représentées les différentes APD concernées. Sans doute, les critères restent à fixer mais cette solution nous apparaît nécessaire au moment où certaines autorités se disputent la compétence de régler certains litiges, invoquant en particulier la primauté de l'effet utile du RGPD sur le critère certes un peu formel du lieu de l'établissement principal.

4. L'ajout de compétences décisionnelles et administratives aux seules compétences d'avis et d'*ombusdman* initialement confiées aux commissions de protection de la vie privée introduit un risque que, dès 1980, le commissaire canadien Flaherty[11] dénonçait. Nos traditionnels « chiens de garde » de la vie privée ne risquent-ils pas sous le poids des textes, de leur responsabilité de juges et de policiers de se transformer en administrateurs de textes et en comptables des résultats de leur travail. À cet égard, on souligne en ce sens le hit-parade des sanctions infligées aux plateformes, la multiplication des notes, des lignes directrices et autres instruments d'interprétation et de mise en œuvre administrative des textes mais, à l'inverse, on regrette que, depuis l'entrée en vigueur du RGPD, peu de codes de conduite aient été négociés avec les secteurs d'activités, l'absence de dialogue avec les « stakeholders » et surtout les détachés à la protection des données dont l'impact sur le fonctionnement de l'entreprise ou de l'administration n'a jamais été évalué. Ne serait-il pas bon que nos autorités s'ouvrent et sortent de leurs tours d'ivoire et de leurs zones de confort ?

II. L'AMPLEUR DU DOMAINE D'APPLICATION

5. À cet égard, on distinguera les domaines d'application *ratione personae, ratione materiae* et *ratione loci*, couverts par le texte. Le RGPD entend s'appliquer à tous les traitements de données à caractère personnel ayant un impact sur les personnes résidentes sur le territoire de l'Union européenne, hormis ceux visés par la directive « Police » et autres exceptions en des domaines exclus de la compétence européenne.

6. En ce qui concerne le domaine d'application *ratione materiae* et sans vouloir analyser à ce stade[12] l'interprétation de plus en plus large de la notion de données à caractère personnel, notons que le texte applique les mêmes devoirs et obligations, certes parfois à interpréter proportionnellement en matière de sécurité, à tous les traitements. L'idée est de soumettre tout traitement à un même régime, qu'il s'agisse des principes des articles 5 et 6,

[11] « 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 voir le second rôle faire oublier le premier » ; Y. Poullet, « 50 ans de législations européennes de protection des données – Hier, aujourd'hui et demain », in B. Bévière-Boyer et D. Dibie (dir.), *Numérique, droit et société*, Paris, Dalloz, 2022, p. 32. À propos de la vision de Flaherty sur les autorités de protection des données, lire : D. Flaherty, « Visions of Privacy : Past, Present, and Future », in C.J. Bennett et R. Grant (dir.), *Visions of Privacy : Policy Choices for the Digital Age*, University of Toronto Press, 1999.

[12] Voy. *infra*, n^os^ 14 et s.

des obligations diverses du responsable du traitement, des droits de la personne concernée et des flux transfrontières. Une seule exception est introduite par les articles 35 et 36 qui imposent le devoir d'un « Privacy Risk Assessment » (PIA) et de notification, en cas de « risques élevés »[13]. L'analyse d'impact est imposée lorsque le traitement présente un « risque élevé », « en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement »[14].

Cette disposition nous paraît judicieuse même s'il faut reconnaître que dans la pratique, les évaluations requises sont rarement effectives, considérées comme une charge administrative et confiées à des consultants externes. Quoi qu'il en soit, le PIA annonce l'approche par les risques promue depuis par le projet de législation sur l'intelligence artificielle (« AI Act »)[15]. Ce dernier suit le principe de proportionnalité qui doit guider toute législation européenne. Il repose sur une réglementation à géométrie variable suivant le degré de risques présentés par les applications technologiques de l'intelligence artificielle (« IA »). Ainsi, le texte interdit ce qu'il considère comme des pratiques illégales de l'IA (article 5) ; soumet à des obligations spécifiques de transparence pour certaines applications cachées, en particulier la reconnaissance par l'IA des émotions (article 52) ; soumet les applications dites « à haut risque » à un système d'évaluation, de contrôle et de gestion (article 62) et, enfin, abandonne à l'autoréglementation du marché les autres applications présentant un risque minime. *Mutatis mutandi*, ne peut-on prévoir que les obligations à charge du responsable du traitement varient en fonction des risques dont la gravité doit tenir compte de divers facteurs cumulés ou non et liés à la finalité des traitements, les catégories de données traitées, les technologies de traitement utilisées, l'impact du traitement sur les personnes concernées, le nombre de personnes concernées, etc. ? Sans doute, la riche liste reprise à l'annexe 3 de la proposition de règlement pourrait inspirer la révision du RGPD. Ainsi, outre l'obligation d'un PIA, la nomination d'un délégué à la protection des données à caractère personnel (« DPO »), l'obligation d'utiliser des systèmes de sécurité certifiés, l'existence d'un organe ayant compétence d'accueillir les demandes d'explication des décisions prises et, le cas échéant, les recours contre ces décisions, le futur législateur pourrait imaginer, au regard des risques particulièrement élevés liés à certains traitements ou à certains acteurs, des interdictions, des limitations de traitement ou des autorisations particulières des autorités de protection des données. Nous reviendrons[16] sur le régime particulier des « gatekeepers », ou « contrôleurs d'accès », selon l'appellation retenue par le DMA[17], ou la catégorie plus restreinte des « very large platforms of information or communication », selon l'appellation retenue par le DSA[18].

13 Sur le PIA et l'intérêt de cette disposition précurseur de l'approche suivie par la proposition de législation européenne sur l'intelligence artificielle, lire notre réflexion, « L'analyse d'impact relative à la protection des données ou plutôt le Privacy Impact Assessment, une révolution non sans lendemain à l'heure de l'intelligence artificielle ? », in C. Castets-Renard et J. Eynard (dir.), *Un droit de l'intelligence artificielle – Entre règles sectorielles et régime général*, Bruxelles, Larcier, 2023, p. 631.

14 Article 35.1 du RGPD.

15 Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle), COM/2021/206 final, Bruxelles, 21 avril 2021 (ci-après « AI Act »). La proposition est toujours en cours de discussion. De multiples amendements sont proposés.

16 Voy. *infra*, n° 19.

17 Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique, *J.O.*, L 265, 12 octobre 2022 (ci-après « DMA »).

18 Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché

7. *Ratione personae*, le constat est le même : uniformité de traitement pour tous les responsables du traitement. On note une exception mais dont l'importance est bien relative : la disposition portant sur la tenue d'un registre des traitements exempte de cette obligation les PME, en raison de la taille du responsable du traitement (article 30.5). Cette généralisation des mêmes obligations inquiète au vu de la lourdeur et du coût que peut représenter la mise en œuvre du cadre réglementaire pour certains responsables ou pour certains traitements. Ainsi, la question du droit d'accès représente dans une grosse entreprise disposant de systèmes performants de contrôle d'accès, de gestion, de traçage des données, un coût peu important. Il n'est pas évident que la situation soit la même pour une entreprise de petite taille, qui répondra sans doute avec retard à la même demande d'accès. Se pose dès lors la question de la proportionnalité des charges imposées par le RGPD lorsque le responsable du traitement est une PME. Des textes récents à propos de la réglementation des données, comme le DSA[19], l'AI Act[20], le Data Act[21] exemptent les « PME » de toute ou partie des obligations mises en place par ces textes, considérant à la fois la lourdeur de ces dernières mais également les moindres risques liés aux activités des entreprises de moindre taille, à moins qu'elles ne soient des filiales ou voient leurs comportements dictés par des groupes puissants dont elles relèvent. Cet argument rejoint l'approche par les risques déjà développée[22].

8. *Ratione loci*, le RGPD impose sa loi bien au-delà des frontières européennes. Au-delà des dispositions élargies sur son application dite « extraterritoriale » à tout traitement qui « vise » les résidents européens, on sait que la contrainte de la protection adéquate en cas de flux transfrontières offerte par le pays ou l'entreprise destinataire, contrainte reprise aux articles 44 et suivants, a été nettement renforcée, jurisprudences *Schrems I* et *II*[23]

unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), *J.O.*, L 277/1, 22 octobre 2022 (ci-après « DSA »).

19 Le considérant 41 du DSA indique que : « À cet égard, il est important que les obligations de diligence soient adaptées au type, à la taille et à la nature du service intermédiaire concerné. Le présent règlement définit donc des obligations de base applicables à tous les fournisseurs de services intermédiaires, ainsi que des obligations supplémentaires pour les fournisseurs de services d'hébergement et, plus particulièrement, pour les fournisseurs de plateformes en ligne et de très grandes plateformes en ligne ainsi que de très grands moteurs de recherche en ligne ».

20 Voy. l'article 55 de l'AI Act. Le considérant 73 indique que : « Afin de promouvoir et de protéger l'innovation, il est important que les intérêts des petits fournisseurs et utilisateurs de systèmes d'IA bénéficient d'une attention particulière. Pour atteindre cet objectif, les États membres devraient prendre des initiatives à l'intention de ces opérateurs, notamment en matière de sensibilisation et de communication d'informations. En outre, les intérêts et les besoins spécifiques des petits fournisseurs doivent être pris en considération lorsque les organismes notifiés fixent les redevances d'évaluation de la conformité. Les frais de traduction liés à la documentation obligatoire et à la communication avec les autorités peuvent constituer un coût important pour les fournisseurs et d'autres opérateurs, en particulier pour ceux de plus petite envergure ». La même approche favorable aux PME est suivie en droit de la concurrence ou plus précisément en matière de partage des données. Sur ce point, voy. les développements de T. Tombal, *Imposing Data Sharing among Private Actors*, coll. Inf. Law Series, n° 48, Kluwer Law Intern, 2022, pp. 187 et s., n^os^ 173 et s.

21 Voy. les articles 9.2 et 14 de la proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées en matière d'accès équitable aux données et de l'utilisation de celles-ci (règlement sur les données), COM(2022)/0047 final, Bruxelles, le 23 février 2022 (ci-après « Data Act »). Cette proposition toujours en discussion entend fixer les règles de collecte et de partage des données collectées dans le cadre de systèmes d'internet des objets.

22 Voy. not. le DSA qui soumet les « very large online platforms » à des obligations nettement plus lourdes, en raison des « risques systémiques » liés à leur taille.

23 C.J., 6 octobre 2015, arrêt *Maximilian Schrems c. Data Protection Commissioner*, C-362/14 (aff. *Schrems I*) ; C.J., 16 juillet 2020, arrêt *Data Protection Commissionner*

aidant. Il s'agit de passer d'un concept pragmatique ouvert à des solutions d'autoréglementation effective à une exigence d'« équivalence substantielle »[24], menant à un devoir d'examen de l'existence tant d'un droit à un recours judiciaire que du cadre juridique environnant. Ces exigences nouvelles représentent, sur le papier, un plus pour la protection des personnes concernées et accélèrent l'adoption de nouvelles lois dans le monde, y compris aux États-Unis. Elles rencontrent cependant des difficultés pratiques lorsqu'elles sont à apprécier, dans un premier temps du moins, par des responsables du traitement. Par ailleurs, en riposte contre cet « impérialisme réglementaire européen » elles risquent de susciter dans les pays qui nous entourent une réaction négative et l'adoption de lois, fondée sur la souveraineté de tels pays, comme on le voit avec l'*US Cloud Act*[25]. Par ailleurs, on sait combien, dans le cadre de la 3e voie européenne[26] qui caractérise la stratégie européenne de développement du numérique, la protection des données est devenue le symbole des valeurs européennes et une garantie pour la confiance des

c. Facebook Ireland Ltd et Maximilian Schrems, C-311/18 (aff. *Schrems II*).

24 Dans ses conclusions, l'avocat général relève que : « 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 » : av. gén. M. Henrik Saugmandsgaard Øe, concl. préc. C.J., 16 juillet 2020, arrêt *Data Protection Commissionner c. Facebook Ireland Ltd et Maximilian Schrems*, C-311/18, point 112. Dans son premier arrêt, la Cour avait déjà indiqué que : « 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 » ; C.J., 6 octobre 2015, arrêt *Maximilian Schrems c. Data Protection Commissioner*, C-362/14, point 73.

25 Le Cloud Act ou de manière complète « Clarifying Lawful Overseas Use of Data Act (H.R. 4943) » est une loi fédérale américaine et qui a été votée en 2018 dans le cadre de l'acceptation du Consolidated Appropriations Act, 2018 (PL 115-141, Division V). Cet instrument autorise les agences américaines d'exécution des lois à exiger que les entreprises technologiques américaines donnent accès aux données stockées sur leurs serveurs, peu importe que les données soient localisées aux États-Unis ou ailleurs. L'Union européenne envisage de donner aux autorités policières ou de renseignements le droit d'avoir accès aux données des entreprises peu importe leur lieu d'établissement dès que l'affaire concerne un délit ou crime dont les victimes sont situées en Europe ; proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale (« e-evidence Act »), COM/2018/225 final. Sur le choc de ces deux approches, lire la thèse en voie de publication de H. H. Abraha, Faculté de droit, Université de Malte, octobre 2021.

26 Cette « troisième voie » européenne, distincte à la fois de celle chinoise et de celle américaine, repose sur la volonté, exprimée à de nombreuses reprises par les autorités européennes, 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, document à la base de cette politique qui marque la troisième voie européenne ; White Paper on Artificial Intelligence : A European approach to excellence and trust, COM(2020) 65 final, 19 février 2020. 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 ».

citoyens européens. Cette invocation cache mal le fait que les textes récents adoptés ou en voie d'adoption en matière de réglementation des données tels que le Data Governance Act[27], le Data Act ou l'AI Act sacrifient certes légèrement mais certainement la cause de la protection des données à une logique de *data sharing*, nécessaire au développement d'une économie européenne de la donnée comme le notent les avis conjoints du CEPD et de l'EDPB à leur propos[28].

III. LE RGPD ET SON ADÉQUATION AUX TECHNOLOGIES ÉMERGENTES

9. Notre société digitale se voit, depuis la publication du RGPD, envahie d'applications nées de l'utilisation de technologies dites « disruptives », dans la mesure où ces applications, ou certaines d'entre elles, entraînent une modification profonde du vivre ensemble. Au premier rang figurent les applications d'intelligence artificielle dites de « machine learning », que l'on songe à celles de reconnaissance faciale, à la voiture intelligente, aux d*eepfakes* et à ce microciblage qui est le corps même du *business model* des plateformes[29] et permet la manipulation des internautes. L'intelligence artificielle se nourrit, entre autres, des données collectées via l'internet des objets, technologie qui, par le caractère nano de ces « terminaux », se loge au creux de nos objets les plus familiers, au centre de nos salons, dans les murs de nos entreprises, sur nos emballages de produits de consommations et à l'intérieur de nos corps et renseigne le collecteur des données – ou ceux à qui il les transmet – d'informations sur notre consommation, présence, santé et autres. L'IA est à la fois infinie mémoire enfouie dans les big data, regardant vers le futur, elle est également instrument puissant de prédictions, qui apparaissent comme autant de vérités sorties des ordinateurs[30].

27 Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données), *J.O.*, L 152/1, 3 juin 2022 (ci-après « DGA »).

28 *Cf.* avis conjoint 03/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données, 10 mars 2021, disponible sur : https://edpb.europa.eu/system/files/2021-09/edpb-edps_joint_opinion_dga_fr.pdf ; avis conjoint 2/2022 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données, 4 mai 2022, disponible sur : https://edpb.europa.eu/system/files/2023-03/edpb-edps_jointopinion_2022-02_data_act_proposal_fr.pdf et avis conjoint 05/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle, 18 juin 2021, disponible sur : https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_fr.pdf.

29 Sans vouloir détailler ici ce *business model*, notons que la gratuité pour l'utilisateur final de nombre de services sur l'internet s'explique par les redevances publicitaires que les plateformes peuvent obtenir en permettant le placement le plus adéquat de leurs publicités aux offreurs de services et de produits et en retenant l'attention des internautes sur les pages accessibles suivant les règles de l'« économie de l'attention », développée par le prix Nobel H. Simon. Pour ce faire, les plateformes et les serveurs présents sur le *web* développent grâce à des technologies de l'IA travaillant sur les données collectées par les systèmes de *webtracking* (cookies et autres) des mécanismes de microciblage permettant de profiler au plus près leurs « internautes » et de leur offrir les messages et publicités correspondant à leurs goûts. Sur ces points, lire N. Bontridder et Y. Poullet, « La "cancel culture", la technologie et le rôle des plateformes à l'aune de la liberté d'expression », *J.T.*, 2022, pp. 661 et s.

30 Selon B. Schroder, « Nous sommes maintenant capables de résoudre de toutes nouvelles classes de problèmes, telles que la reconnaissance d'image ou la transcription de la voix. Nous pouvons prédire des événements non modélisables. Par exemple, Cornell University détecte la survenance de l'état dépressif de patients bipolaires en analysant les changements dans la frappe de messages sur l'écran d'un smartphone (Z. Bokai *e.a.*, *KDD'17 Proceedings of the 23rd ACMSIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 747-755, ACM). Un algorithme de Microsoft prévoit un diagnostic futur de cancer du pancréas ou de poumon par l'analyse de

Comment ne pas évoquer également la technologie de la *blockchain ?* Cette technologie confie à la seule décision privée et à la sécurité assurée par le réseau et à sa décentralisation le soin de garantir l'authentification d'un document, transaction ou non, en supprimant l'intervention des tiers de confiance et, liée à cette intervention, le cas échéant, les contrôles des États[31]. Plus inquiétante encore, l'irruption des technologies dites NBIC[32] autorisent dès aujourd'hui et plus encore demain, la manipulation génétique et l'augmentation de nos capacités. Se profilent la possibilité de l'homme augmenté et la crainte y corrélée d'une société à deux vitesses. Sans doute, à moyen terme, devons-nous évoquer les applications promises par Meta, combinant 3D et intelligence artificielle, qui nous permettront à travers des avatars de dialoguer en virtuel comme nous pourrions le faire physiquement présents. On peut craindre que cette technologie augmente notre addiction et la possibilité accrue de manipulations. Notre propos est de nous interroger sur l'adéquation du RGPD par rapport à ces applications nouvelles. Cette interrogation se fera en deux temps. Le premier s'inscrit dans une analyse des questions techniques posées par ces technologies à l'application des dispositions du RGPD. C'est à cette analyse que sera consacré le présent point. Dans un second temps[33], nous porterons notre attention sur les questions soulevées par ces technologies et non abordées par le RGPD et qui interrogent sur la portée du texte, en même temps que sur le rôle d'une instance de protection des données par rapport à ces dimensions nouvelles.

10. À propos du premier point, nous nous limitons aux seuls cas de l'intelligence artificielle, de la *blockchain* et de l'internet des objets. Dans une publication récente relative à l'intelligence artificielle et son encadrement par le RGPD[34], nous soulignions notamment les points d'attention suivants :

– les dispositions du RGPD ne s'intéressent qu'aux seules données à caractère personnel. Or, les données utilisées dans le cadre de beaucoup d'applications concernent tant des données à caractère personnel que des données anonymes[35]. Par ailleurs, les possibilités incroyables de couplage des données conduisent à considérer que les technologies de pseudonymisation et d'anonymisation constituent des garanties parfois insuffisantes pour assurer

l'historique des mots-clés entrés dans un moteur de recherche (J. Paparrizos *e.a.*, "Screening for Pancreatic Adenocarcinoma Using Signals From Web Search Logs : Feasibility Study and Results", *Journal of Oncology Practice* 12, n° 8 [August 01, 2016] 737-744) » ; B. Schroder, *Vie Privée, transparence et démocratie*, Actes du Colloque du REHNAM, Namur le 28 novembre 2019, Y. Poullet (éd.), coll. Cahiers du CRIDS, n° 47, Bruxelles, Larcier, 2020, pp. 67 et s.

31 Sur cette technologie, ses enjeux et les diverses questions juridiques soulevées, lire entre autres, H. Jacquemin, A. Cotiga et Y. Poullet (dir.), *Les blockchains et les smart contracts à l'épreuve du droit,* coll. Cahiers du CRIDS, n° 49, Bruxelles, Larcier, 2020.

32 Les nanotechnologies, biotechnologies, informatique et sciences cognitives (NBIC) sont un champ scientifique multidisciplinaire qui se situe au carrefour des nanotechnologies (N), des biotechnologies (B), des technologies de l'Information (I) et des sciences cognitives (C). Certains utilisent la notion de « grande convergence » pour souligner l'interconnexion croissante entre « l'infiniment petit (N), la fabrication du vivant (B), les machines pensantes (I) et l'étude du cerveau humain (C) » (Wikipedia, *v°* « NBIC », disponible sur : https://fr.wikipedia.org/wiki/Nanotechnologies,_biotechnologies,_informatique_et_sciences_cognitives).

33 Voy. *infra*, point IV.

34 Y. Poullet, *Le RGPD face à l'intelligence artificielle,* coll. Cahiers du CRIDS, n° 50, Bruxelles, Larcier, 2020. Pour un exposé également critique, lire L. Mitrou, « Data Protection, Artificial Intelligence and Cognitive Services : Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"? » (December 31, 2018), disponible sur le site SSRN : https://ssrn.com/abstract=3386914 ou http://dx.doi.org/10.2139/ssrn.3386914.

35 Voy. *infra*, n° 15.

la protection des données. Le risque d'individualisation des données doit faire l'objet d'une attention particulière et des engagements excluant toute tentative de réidentification ou ré-individualisation devraient, dans certains cas, être recommandés voire imposés ;

- le statut du nombre d'acteurs impliqués dans la constitution ou l'implémentation des applications IA est peu clair au regard des classifications du RGPD et que, par ailleurs, les obligations qui naissent des dispositions du RGPD sont limitées aux seuls responsables du traitement et sous-traitants, alors qu'il apparaît important d'imposer certains devoirs aux fournisseurs des éléments d'une application d'IA[36] ;
- l'application des principes de finalité et de compatibilité nécessitera une attention particulière dans la mesure où les applications d'IA permettent très facilement de découvrir de nouvelles finalités et que dès lors les responsables seront tentés d'élargir les potentialités des traitements ;
- les principes de minimisation et de proportionnalité peuvent difficilement être appliqués dans la mesure où leur application va à l'encontre même du fonctionnement des systèmes de *machine learning*. À l'inverse des systèmes experts fondés sur une logique décrite *a priori*, le fonctionnement des systèmes d'IA repose sur des corrélations par définition non prévisibles mais significatives entre les données les plus diverses et riches possible[37]. Ceci dit, on sera attentif à brider les algorithmes, c'est-à-dire à leur imposer certaines contraintes de manière à empêcher des violations de règles de protection des données et à tester sur des données d'entraînement les premiers résultats de manière à éviter des corrélations insensées ;
- la loyauté des traitements d'IA exige une information renforcée et aisée des personnes concernées sur leur existence (en particulier en matière de robots), les catégories de données utilisées, le modèle retenu pour le traitement et l'impact du traitement sur les personnes concernées. Un accès électronique aux données collectées doit être ménagé de préférence directement par la conception même du système ;
- le principe de l'article 22 du RGPD, qui interdit que les personnes concernées soient soumises à des décisions prises exclusivement[38] sur base d'un traitement

[36] À noter cependant le considérant 78 du RGPD indiquant que : « il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données ».

[37] « La prolifération et le traitement de quantités massives de données – présupposés par le phénomène des Big Data et par les solutions robotiques qui s'en nourrissent – entrent en opposition frontale avec les grands principes de protection des données : la minimisation (on ne collecte que les données nécessaires au but poursuivi), la finalité (on ne collecte de données qu'en vue d'un but identifié, déclaré légitime), la limitation dans le temps (les données doivent être effacées une fois le but atteint et ne peuvent être utilisées, sauf exceptions, à d'autres fins que les fins initialement déclarées. Les Big Data c'est au contraire une collecte maximale, par défaut, la conservation illimitée de tout ce qui existe sous une forme numérique, sans qu'il y ait nécessairement de finalité établie *a priori*, puisque l'utilité des données ne se manifeste qu'en cours de route, à la faveur des pratiques statistiques de *datamining*, de *machine learning,* etc. ». A. Rouvroy, « La robotisation de la vie et la tentation de l'inséparation », in H. Jacquemin et A. de Streel (dir.), *L'intelligence artificielle et le droit*, coll. Cahiers du CRIDS, n° 41, Bruxelles, Larcier, 2017, p. 23.

[38] Le mot « exclusivement » est trompeur. Il est en effet facile pour le responsable d'affirmer que le résultat de

automatisé, mérite une extension et une réglementation particulière en matière de système d'intelligence artificielle. Ainsi, comme le réclame dans deux arrêts récents[39] la Cour de justice de l'Union européenne, la transparence ou, au moins, l'explicabilité des traitements d'IA doit être rendue obligatoire lorsqu'il s'agit de systèmes utilisés par l'autorité publique ou de systèmes à hauts risques et le droit à une réelle intervention humaine, disposant des compétences à la fois techniques et décisionnelles, doit être consacré, interdisant dès lors l'utilisation de systèmes fondés sur la technologie de l'apprentissage machine[40].

11. L'application du RGPD aux *blockchains* rencontre de même des difficultés majeures[41]. L'utilisation de la *blockchain*, suivant les multiples formes qu'elle peut prendre, met en jeu nombre d'acteurs sans que l'on puisse déterminer un acteur central : l'utilisateur, qui entend utiliser le système aux fins de réaliser une transaction ou de loger un document ; les nœuds du réseau où seront stockées les traces du document ; les « mineurs » qui ajoutent de nouvelles données pour sécuriser les messages, et ce suivant le protocole du réseau. À ceux-là, s'ajoutent le développeur du logiciel, les fournisseurs des portefeuilles, les « wallet providers », acteurs qui apportent les clés de cryptage des documents mais aussi souvent constituent l'interface avec la plateforme. Bref, il n'est pas évident de déterminer qui est le responsable du traitement. Si c'est l'utilisateur qui détermine les finalités, il a souvent peu de maîtrise sur les moyens. La question de l'information de la personne concernée à propos de

l'application du système IA n'a servi que d'avis susceptible d'être remis en cause par un agent du responsable, préposé à la vérification du bien-fondé des propositions de l'ordinateur. Il importera d'analyser dans quelle mesure la personne humaine chargée d'intervenir à la suite de la proposition sortant de l'ordinateur dispose dans le cadre de son organisation et de la procédure prévue, d'une réelle capacité en temps et en compétence, de s'écarter de la proposition et l'exerce effectivement. On souligne combien cette décision, pour un employé ou un fonctionnaire, de s'écarter des propositions que lui livre la machine ne sera pas chose aisée. Il risque de devoir rendre compte des raisons de l'écart pris avec ce qui apparaît la « vérité sortie de l'ordinateur », en particulier si la décision substituée est suivie de conséquences fâcheuses.

39 Ainsi, les arrêts *Privacy International*, *La Quadrature du Net e.a.*, *French Data Network e.a.*, et *Ordre des barreaux francophone et germanophone* relatifs aux obligations de rétention de données imposées par certains pays aux opérateurs de service de communication et qui soulignent les dangers nouveaux que constituent l'opacité, l'évolution et le risque de biais et de faux positifs liés à l'utilisation de technologies de « machine learning » ; C.J., 6 octobre 2020, arrêt *Privacy International*, C-623/17 ; C.J., 6 octobre 2020, arrêt *La Quadrature du Net e.a. c. Premier ministre e.a.*, aff. jointes C-511/18, C-512/18, C-520/18 et l'arrêt *PNR*, plus sévère encore à propos de l'utilisation de ces technologies : C.J., 21 juin 2022, arrêt *Ligue des droits humains c. Conseil des ministres*, C-817/19.

40 L'arrêt du 21 juin 2022 est particulièrement cinglant à ce propos : « Compte tenu de l'opacité caractérisant le fonctionnement des technologies d'intelligence artificielle, il peut s'avérer impossible de comprendre la raison pour laquelle un programme donné est parvenu à une concordance positive » (point 195). Dans le même ordre d'idées, la Cour ajoute que l'utilisation de technologies d'IA fonctionnant sur la base de l'apprentissage machine serait « susceptible de priver les personnes concernées également de leur droit à un recours juridictionnel effectif […], en particulier pour contester le caractère non discriminatoire des résultats obtenus » (point 195).

41 Parmi la doctrine à ce propos, lire M. Finck, « Blockchain and the General Data Protection Regulation : Can distributed ledgers be squared with European data protection law ? », *Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit*, 2019 ; D.G. Duarte, « An Introduction to Blockchain Technology From a Legal Perspective and Its Tensions With the GDPR », *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law -CIJIC*, 2019, disponible sur SSRN : https://ssrn.com/abstract=3545331 ou http://dx.doi.org/10.2139/ssrn.3545331, en particulier, pp. 42-65 ; A. Delforge et Y. Poullet, « Les blockchains : un défi et/ou un outil pour le RGPD ? », in H. Jacquemin, A. Cottiga et Y. Poullet (dir.), *Les blockchains et les smart contracts à l'épreuve du droit*, coll. Cahiers du CRIDS, n° 49, Bruxelles, Larcier, 2020, pp. 97-135.

l'utilisation d'une *blockchain* comme outil de conservation de ces données est controversée et ne se déduit pas facilement des dispositions du RGPD. On ajoutera les difficultés pour la personne concernée de pouvoir exercer pleinement son droit à l'oubli (article 17). Enfin, les *smart contracts* qui peuvent être liés à la *blockchain* (par exemple, en ce qui concerne le déclenchement d'une indemnisation par une compagnie d'assurances) soulèvent la question de l'application possible de l'article 22 du RGPD.

12. La voie suivie par la proposition de règlement relatif aux dispositifs dits d'internet des objets, le Data Act, mérite d'être soulignée et pourrait inspirer d'autres initiatives relatives à des technologies particulières[42], et ce en raison des risques spécifiques posés par ces technologies. Ainsi, l'article 3 ajoute des informations complémentaires relatives aux produits ou services liés à fournir par celui qui offre le produit ou le service, sans qu'il soit fait mention de sa qualité de responsable du traitement. Le même article exige que « la conception et la fabrication des produits, et la fourniture des services liés, sont telles que les données générées par leur utilisation sont, par défaut, facilement, de manière sécurisée et, lorsque cela est pertinent et approprié, directement accessibles à l'utilisateur »[43]. Ainsi, le droit d'accès n'est plus médiatisé par le responsable du traitement. On note que l'utilisateur, qui souvent sera une personne physique, peut exiger le transfert de ces données à un tiers déterminé et s'opposer à d'autres communications. La proposition (article 5.2) s'oppose à ce que les entreprises fournissant des services de plateforme essentiels désignées comme contrôleurs d'accès puissent être bénéficiaires de ces transmissions[44] et l'article 6 demande au tiers de s'abstenir notamment d'utiliser les données à des fins de profilage[45]. Au-delà, la portabilité des données prévue par l'article 20 du RGPD s'élargit à des obligations d'interopérabilité des systèmes, c'est-à-dire à « la capacité d'au moins deux espaces de données ou réseaux de communication, systèmes, produits, applications ou composants d'échanger et d'utiliser des données afin de remplir leurs fonctions »[46]. Notre propos s'inscrit donc dans la remise en cause d'une approche réglementaire générale et non différenciée des traitements. Nous pensons que les exigences du RGPD ne devraient pas être imposées à tous les traitements, nous croyons que la réglementation de la protection des données doit être modulée par la considération des technologies utilisées de manière à être adéquate aux risques générés par ces technologies et aux solutions qu'elles peuvent fournir dans une approche « privacy by design »[47]… ou plutôt, car les préoccupations se conjuguent, « consumer protection by design ».

42 À cet égard, on notera que la réglementation, via l'article 5.3 de la directive 2002/58/CE (« directive e-Privacy ») en cours de révision, des cookies ou plus largement des méthodes de *webtracking* constituait également une réglementation particulière des technologies de collecte des données liées à la navigation sur le web et ajoutait des garanties complémentaires à celles offertes par le RGPD.

43 Article 3.1 du Data Act.

44 L'article 5.2 du Data Act dispose que : « Toute entreprise fournissant des services de plateforme essentiels dont un ou plusieurs ont été désignés comme contrôleur d'accès, conformément à l'article […] du [règlement XXX] relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques), n'est pas un tiers éligible au titre du présent article ».

45 Article 6.2 (b) du Data Act.

46 Article 2.19 du Data Act.

47 Article 25 du RGPD. Pour prendre un autre exemple, l'article 26.1 du DSA précité prévoit que le fournisseur de plateformes en ligne présentant de la publicité sur ses interfaces doit veiller à ce que, pour chaque publicité spécifique présentée à chaque destinataire individuel, les destinataires du service puissent de manière claire, précise, non ambiguë et en temps réel se rendre compte que les informations sont de la publicité, identifier la personne physique ou morale

IV. LA QUESTION DES CONCEPTS DU RGPD AU REGARD DE LA RÉALITÉ ACTUELLE

13. Le RGPD définit son champ d'application par la notion de données à caractère personnel, parmi lesquelles il distingue des « catégories particulières de données » ; les données sensibles des articles 9 et 10. Il envisage la réglementation d'acteurs particuliers : les responsables du traitement et les sous-traitants. Notre propos interroge ces concepts, à la lumière d'opinions ou décisions récentes tant des autorités de protection des données que de la Cour de justice de l'Union européenne.

A. La notion de données à caractère personnel

14. La notion de données à caractère personnel s'étend bien au-delà des données permettant au responsable du traitement, moyennant des efforts raisonnables, de retrouver directement ou indirectement l'identité de l'individu concerné. Plusieurs avancées à cet égard. Dans une affaire récente, dite IAB[48], l'autorité belge de protection des données a considéré que « tant que des informations, en raison de leur contenu, de leur finalité ou de leur effet, peuvent être reliées à une personne physique identifiée ou identifiable par des moyens pouvant être raisonnablement mis en œuvre, et ce, que les informations à partir desquelles la personne concernée peut être identifiée soient détenues entièrement par le même responsable du traitement ou en partie par une autre entité, ces informations doivent être considérées comme des données à caractère personnel »[49]. Autre avancée, désormais il suffit pour que la donnée soit considérée comme donnée à caractère personnel que la donnée collectée permette l'individualisation, c'est-à-dire l'impact auprès d'une personne X, dont par ailleurs l'identité n'est plus recherchée[50]. Les tenants de la « Group Privacy »[51]

pour le compte de laquelle la publicité est présentée, identifier la personne physique ou morale qui a payé pour la publicité et déterminer les informations utiles, qui doivent être directement et facilement accessibles à partir de la publicité, concernant les principaux paramètres utilisés pour déterminer le destinataire auquel la publicité est présentée et, le cas échéant, la manière dont ces paramètres peuvent être modifiés.

48 Autorité de protection des données, décision sur le fond 21/2022 du 2 février 2022, n° de dossier DOS-2019-01377, cette décision a fait l'objet d'un appel, qui elle-même a adressé à la C.J.U.E. certaines questions préjudicielles. Sur cette décision, lire entre autres le commentaire de J. Eynard et M. Prudet, « Une opaque publicité : au sujet des enchères en ligne », obs. sous APD, décision n° 21/2022 du 2 février 2022, *R.D.T.I.*, 2022/3-4, pp. 117-133.

49 Autorité de protection des données, décision sur le fond 21/2022 du 2 février 2022, p. 67.

50 Il s'agit de passer, selon le terme heureux de C. de Terwangne, de l'identification d'une personne, c'est-à-dire d'une possibilité de retrouver les éléments de son identité légale (nom, prénom, adresse, etc.), à l'individualisation, c'est-à-dire la capacité de rapporter à un individu singulier des données, sans que les éléments de son identité légale soient connaissables. Ainsi, le tag RFID porté par une personne X se baladant dans un supermarché, ne permettra sans doute pas l'identification de son porteur mais permettra de le localiser au sein de ce supermarché, de tracer, le cas échéant, ses précédents achats, voire de connecter de telles informations à celles résultant de ses habitudes de *surfing ;* C. de Terwangne, « Définitions clé et champ d'application du RGPD », in C. de Terwangne et K. Rosier (dir.), *Le Règlement général sur la protection des données (RGPD/GDPR), Analyse approfondie,* coll. Cahiers du CRIDS, n° 44, Bruxelles, Larcier, 2018, pp. 63 et s.

51 L. Taylor, L. Floridi et B. van der Sloot (éd.), *Group Privacy : new challenges of data technologies*, Dordrecht, Springer, 2017. Voy. aussi : « In conclusion, the first of the two reasons underlying the creation of the FIPs and the early European data protection rules, as separated from the right to privacy, was that personal data are often neither private nor sensitive. Currently, this is even more so and even non-identifiable information can be connected and harvested through the use of advance techniques in order to create profiles. Consequently, to cope with the fact that personal data are less and less linked to the individual subject, the definition of personal data has been widened and broadened over time. 24 However, the second principle, which moved the concept of subjective rights

vont plus loin encore. L'analyse du fonctionnement des systèmes de profilage par application de technologies d'intelligence artificielle de type « machine learning » démontre que ce qui est visé par l'utilisation de ces techniques est non plus l'individu mais le groupe, sans par ailleurs que les caractéristiques de ce groupe ne soient transparentes. Le rapprochement de la personne individuelle au groupe est secondaire et s'opère de manière automatisée, instantanée et opaque. Dans ce contexte, les défenseurs de la « Group Privacy » estiment que le premier souci doit être la protection des groupes et non plus des individus, qui à la limite peuvent se trouver heureux d'être rangés dans tel groupe sans prendre en considération la légitimité de ce groupage[52].

De cette préoccupation, nous en rapprochons une autre, celle de la dimension de plus en plus non individuelle des données. Le cas des données génétiques peut être cité à ce propos mais au-delà, il est utile de pointer que les données échangées en particulier dans les réseaux sociaux et ou celles reprises dans les moteurs de recherche ou affichées par les « generative AI »[53] concernent souvent bien d'autres personnes que les seuls auteurs des messages ou les personnes pointées par l'interrogation du client du moteur de recherche ou du « generative AI ». La volonté européenne, sans doute bien légitime[54], de développer le partage des données voire de l'imposer si tel est le souhait de la personne concernée comme l'affirme l'article 20 du RGPD ou l'article 5 de la proposition Data Act, soulève une difficulté lorsque la décision de partage émane d'une des personnes concernées mais pourrait rencontrer des objections de la part des autres personnes concernées indirectement visées par cette décision[55].

15. Par ailleurs, certains mettent en cause la notion même de données anonymes[56]. Le

and the individual's right to control over personal data to the background, in favour of general obligations of fairness and reasonableness for the data controller, is increasingly lost » ; 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*, vol. 4, 2014, p. 309.

52 L. TAYLOR, L. FLORIDI et B. VAN DER SLOOT (éd.), *op. cit.*, pp. 10 et s.

53 Comme Chat GpT, ce que le Parlement dans son compromis du 9 mai, appelle « Foundation model » et définit de la manière suivante : « Foundation model = an AI model that is trained on broad data at scale, is designated for generality of outputs and can be adapted to a wide range of distinctive task » ; article 3.1 sous c), du compromis de l'IA Act : Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206-C9-0146/2021-2021/0106(COD), P9_TA(2023)0236).

54 Tant pour permettre de renforcer l'autodétermination des personnes concernées que pour permettre un marché plus concurrentiel.

55 L'article 20.4 du RGPD se contente d'affirmer que : « Le droit visé au paragraphe 1 ne porte pas atteinte aux droits et libertés d'autrui ». Sur ce texte et sa difficile interprétation, lire Groupe de travail « Article 29 » sur la protection des données, Lignes directives relatives au droit à la portabilité des données, WP 242 rev.01, 5 avril 2017, p. 11.

56 Lire en ce sens, les propos de A. Rouvroy : « Les informaticiens le savent : l'anonymat, par exemple – une notion dont les juristes se servent pour circonscrire le champ d'application des régimes de protection des données personnelles (il suffit qu'une donnée soit anonyme pour qu'elle sorte du champ d'application de la loi) – est une notion obsolète à l'heure des Big Data. Aujourd'hui, en raison de la masse des données avec lesquelles elle peut être reliée, toute donnée numérique – aussi impersonnelle, triviale, publique, anonyme soit-elle originairement – transpirant de nos actions et interactions en ligne et hors ligne est potentiellement susceptible de contribuer à nous (ré-)identifier. Les possibilités illimitées de croisements de données anonymes et de métadonnées (données à propos des données) permettent, avec plus ou moins de facilité, pour des coûts plus ou moins faibles, de réidentifier les personnes quand bien même toutes les données auraient été "anonymisées" » ; A. ROUVROY « L'*homo Juridicus* est-il soluble dans les données ? », in E. DEGRAVE, C. DE TERWANGNE, S. DUSOLLIER et R. QUECK

maniement des algorithmes d'intelligence artificielle par le croisement de multiples données à caractère personnel et anonymes peut, dans des cas de plus en plus nombreux, désanonymiser la donnée. La remarque vaut *a fortiori* pour des données «pseudonymisées». En matière de profilage, comment ne pas mettre au même rang que les données à caractère personnel, celles anonymes qui ajoutent une plus-value à la constitution du profil des personnes concernées[57] ? Les catégories particulières de données (dites «sensibles») se sont multipliées avec le RGPD. Traditionnellement, elles se définissent par la nature même des contenus. La jurisprudence de la Cour de justice de l'Union européenne[58] a récemment corrigé cette approche, en lui préférant une approche par la finalité du traitement[59]. Cette question des données sensibles rejoint celle de la discrimination. À cet égard, on note que le profilage permis par l'utilisation du numérique et en particulier de l'IA, grâce à ses «vertus» prédictives, non seulement multiplie les risques de discrimination fondés sur d'autres critères que ceux traditionnellement liés aux données sensibles (ainsi, les personnes ayant telle habitude de *surfing* sont jugées comme des candidats à tel emploi peu valables) mais également vise d'abord des groupes de personnes[60]. Nous pensons que les autorités indépendantes en charge de la protection des données devraient mieux collaborer avec les autorités en charge de l'égalité des chances

(éd.), *Droit, normes et libertés dans le cybermonde, Liber Amicorum Yves Poullet*, coll. Cahiers du CRIDS, Bruxelles, Larcier, 2018, p. 428. Même constatation dans la déclaration du Groupe de travail «Article 29» sur les mégadonnées: «Par ailleurs, les opérations de traitement de mégadonnées n'impliquent pas toujours l'exploitation de données à caractère personnel. Néanmoins, la conservation et l'analyse de gros volumes de données à caractère personnel dans des environnements de mégadonnées requièrent une attention et des précautions particulières. Il est en effet possible d'identifier des profils d'individus précis, notamment parce qu'on dispose de davantage de puissance de calcul et de moyens accrus d'exploration des données» ; Groupe de travail «Article 29», Déclaration concernant l'impact du développement des mégadonnées sur la protection des individus à l'égard du traitement de leurs données à caractère personnel dans l'Union européenne, WP 221, 16 septembre 2014. Voy. égal., l'article de D. Gray et D. Citron, «The right to quantitative privacy», *Minnesota Law Review,* n° 98, 2013, pp. 62 et s.

57 *Cf.* à ce propos, Conseil de l'Europe, Protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage, CM/Rec(2021)8 (2021), 13 avril 2021. On notera également sur la question du profilage, EDPB, Lignes directrices 8/2020 sur le ciblage des utilisateurs de médias sociaux, 13 avril 2021. À noter dans le même sens, l'affirmation de la Commission européenne qui dans ses lignes directrices relatives au règlement concernant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, affirme que: «si les données à caractère non personnel et les données à caractère personnel sont "inextricablement liées", les droits et obligations en matière de protection des données découlant du RGPD s'appliquent pleinement à l'intégralité de l'ensemble de données mixtes, même lorsque les données à caractère personnel ne représentent qu'une petite partie de l'ensemble de données» ; COM(2019) 250 final, 29 mai 2019.

58 C.J., 1er août 2022, arrêt *OT c. Vyriausioji tarnybinės etikos komisija*, C-184/20.

59 On rapprochera de cette proposition, celle qui peut être déduite de l'article 9.1 du RGPD: «le traitement des données à caractère personnel *qui révèle* (*et non qui révèlent*, nous soulignons) l'origine raciale, les opinions politiques…». Ainsi, c'est le traitement qui révèle l'origine raciale ou ethnique (exemple: sélectionner tous les noms terminant en «SKI» de façon à retrouver l'origine polonaise des personnes concernées), les opinions politiques (présence dans la rue à une manifestation d'un parti politique), l'appartenance syndicale, les convictions religieuses, la santé ou la vie sexuelle. Le scandale *Cambridge Analytica* témoigne du fait que des communications triviales sur Facebook, les réponses à des questions dont la teneur était tout sauf politique peuvent être traitées par des systèmes d'intelligence artificielle et peuvent révéler ou en tout cas prétendre révéler les «préférences» politiques des individus. Les mots choisis pour l'interrogation d'un moteur de recherche peuvent révéler l'état de santé de l'internaute.

60 Sur ces deux points, lire la thèse de L. Naudts, *Fair or Unfair differentiation – Reconsidering the Concept of Equality for the regulation of Algorithmically Guided decision-Making,* Thesis, Faculty of Law, KUL, janvier 2023 (en voie de publication).

afin d'éviter ces nouvelles formes de discrimination. On ajoute que si la lutte contre les formes traditionnelles de discrimination, qui découlent de la liste des catégories particulières de données à l'article 9.1, est prise en charge par des associations ayant pignon sur rue, il n'en est pas de même vis-à-vis de ces nouvelles formes de discrimination.

16. Une dernière réflexion, déjà la directive 2002/58/CE concernant la vie privée et les communications électroniques[61] (directive «e-Privacy») avait étendu la protection des données de communication électronique aux personnes morales[62]. Cette extension de la protection s'expliquait d'abord par la difficulté de distinguer la personne morale et la personne physique qui se cache derrière la personne morale. En protégeant la première, on entendait également protéger la seconde. Une autre explication de cette assimilation était le déséquilibre informationnel que pourrait générer l'utilisation des données de communication de l'utilisateur par l'opérateur du service de communication et l'utilisateur. Les récents textes européens cités, en projet ou déjà votés, entendent prolonger cette extension de la protection aux personnes morales, lorsqu'elles sont utilisatrices d'un service qui risque, par le traitement des données qu'il autorise, de nuire grandement à la liberté d'entreprendre ou d'association de cette dernière. Ainsi, le DMA reconnaît des droits aux utilisateurs professionnels vis-à-vis des contrôleurs d'accès, droits semblables à ceux octroyés aux individus dans le cadre du RGPD, ainsi, le droit à la portabilité (articles 6 et 7) et le droit d'accès à leurs données (articles 6, 10 et 11). On ajoute des obligations d'information pour les «responsables du traitement» (en l'occurrence, les contrôleurs d'accès) calquées sur celles du RGPD et des restrictions imposées à l'utilisation des données auprès des entreprises utilisatrices[63]. La proposition de Data Act ne distingue pas, parmi les utilisateurs finaux[64], les personnes physiques et celles morales (article 2.5) pour donner à l'une comme à l'autre des droits comme celui d'accéder aux données générées par l'utilisation du produit et des services liés au système d'IoT mis en place (article 3), comme le droit de choisir le destinataire de ses données (article 5), etc.

Qu'on nous comprenne bien. Certes, le déséquilibre économique né des capacités de collectes d'information et de leurs traitements y compris à des fins de prédiction met en cause les libertés économique ou d'association de personnes morales et il est donc utile de réglementer la protection de ces dernières en appliquant certaines règles déjà existantes en matière de protection des données, sans pour autant confondre les objectifs et les autorités en charge de leur protection. Les banques ou encore les assureurs disposent, grâce au numérique et à l'IA en particulier, d'outils puissants

61 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.C.E.*, L 201, 31 juillet 2002 (ci-après «directive vie privée et communications électroniques»).

62 Article 1er de la directive de 2002 vie privée et communications électroniques.

63 Article 6.2 du DMA: «Le contrôleur d'accès n'utilise pas, en concurrence avec les entreprises utilisatrices, les données, quelles qu'elles soient, qui ne sont pas accessibles au public, qui sont générées ou fournies par ces entreprises utilisatrices dans le cadre de leur utilisation des services de plateforme essentiels concernés ou des services fournis conjointement aux services de plateforme essentiels concernés, ou à l'appui de ceux-ci, y compris les données générées ou fournies par les clients de ces entreprises utilisatrices».

64 Il va de soi que si l'utilisateur final utilise le produit IoT pour collecter des données vis-à-vis de personnes physiques (par exemple, l'entreprise vis-à-vis de ses employés, le centre commercial par rapport à ses clients), le RGPD s'appliquera.

capables de prédire ou, en tout cas d'estimer, l'avenir d'une entreprise ou d'une filiale voire de la « condamner » à travers des *rankings* négatifs[65]. Protéger en particulier les entreprises petites et moyennes contre ces traitements de profilage semble nécessaire, en ce compris pour les travailleurs y occupés et les territoires où ces entreprises sont installées. Affirmant cela, nous ne prônons pas l'extension du RGPD et de sa protection aux associations et personnes morales. Il y va d'une autre logique plus proche du droit de la concurrence et en particulier de la liberté d'entreprendre que des droits et libertés du citoyen[66]. Cela dit, que les droits subjectifs d'accès, de rectification, d'effacement copiés de ceux conférés par le RGPD aux individus soient octroyés aux personnes morales en situation de dissymétrie informationnelle non dans le cadre du RGPD mais bien d'une réglementation différente à portée plus économique et sociale serait utile voire nécessaire à l'heure où les prédictions de l'IA se généralisent.

B. Les acteurs : responsables de traitement et sous-traitants et…

17. L'identification des responsables de traitement soulève une difficulté lorsque la réalisation d'une application implique l'intervention d'une « supply chain » avec de nombreux acteurs. Ainsi, à propos des *blockchains* ou des écosystèmes qui entourent des applications liées à l'internet des objets et généralement de l'intelligence artificielle, à côté de l'utilisateur de l'application (la banque, l'administration…), s'ajoutent des concepteurs, des fournisseurs d'algorithmes, de données, des testeurs, ou dans l'exemple de la *blockchain* ou autres applications totalement décentralisées, de milliers de lieux de stockage… autant d'acteurs qui pèseront sur la définition des finalités et/ou des moyens du traitement. Les seules catégories de responsable du traitement et de sous-traitant suffisent-elles ? 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.

18. Par ailleurs, on note que la qualification de responsables conjoints semble de plus en plus constituer une solution pour les juges, en particulier de Luxembourg, qui, à défaut de pouvoir trouver un responsable, préfèrent en cibler plusieurs, au motif que c'est l'addition de leurs apports qui permet et explique le traitement. En particulier, la notion de « responsable conjoint » introduit par l'article 26 du RGPD semble pouvoir être utilisée également dans le contexte des montages nécessaires à l'exploi-

[65] On évoquera dans ce sens les droits nouveaux accordés par le règlement européen (UE) 2019/1150 qui entend protéger l'entreprise utilisatrice des services de la plateforme, notamment en ce qui concerne les pratiques de *ranking ;* règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, *J.O.*, L 186/57, 11 juillet 2019.

[66] « Importantly, it should be outlined from the outset that while the word "empowerment" is used for both individuals and small business users in my analysis, this word should not be understood exactly in the same way in these two situations. Indeed, as outlined above "empowering" individuals means giving them more control over their data, in order for them to be able to take appropriate decisions about all aspects of their lives. On the other hand, initiatives "empowering" small business users should be understood in a narrower way, as a solely economic empowerment to operate freely and efficiently on the market, which derives from their freedom to conduct a business » ; T. Tombal, *op. cit.*, p. 188.

tation des systèmes IA[67]. Les récentes lignes directrices sur le « ciblage des utilisateurs des réseaux sociaux » énoncées par l'EDPB[68] confirment la jurisprudence de la Cour et examinent en particulier les différentes méthodes de ciblage de la clientèle utilisées par les entreprises et les plateformes de réseaux sociaux, pour conclure à l'existence d'une responsabilité conjointe de la plateforme qui, soit, fournit les profils demandés par l'entreprise, soit, aide à la sélection de ceux-ci sur base des critères retenus par cette dernière et permet l'accès sélectif à la base de données détenue par la plateforme.

Cette extension de la catégorie de responsables conjoints certes contrainte par l'absence de qualification idoine par le RGPD des différents acteurs de la *supply chain* doit-elle être suivie ? Peut-on qualifier comme responsables conjointes les entreprises mettant à disposition de clients des infrastructures qui permettront à ces dernières de développer les traitements répondant à leurs objectifs ? Cette qualification suppose, me semble-t-il, une réelle communauté d'intérêts, comme cela est le cas lorsque Google Spain et Google Int. Ltd coopèrent. Est plus contestable cependant, et c'est le cas dans les affaires européennes *Fashion ID*[69] et *Wirtschaftsakademie*[70] ou l'affaire belge *IAB*[71], la qualification de responsables conjoints lorsque la coopération n'existe pas entre deux entreprises liées par un objectif commun mais résulte de la mise à disposition et de l'utilisation d'un service que l'infrastructure partagée rend disponible à une clientèle variée. Ne faut-il pas, plutôt que d'appréhender par la co-responsabilité de l'opérateur de l'infrastructure du fait de l'utilisation par un tiers, déterminer une responsabilité propre de cet opérateur, eu égard aux risques que son infrastructure crée pour les personnes concer-

67 Ainsi, dans l'affaire *Fashion ID (entreprise de vêtements en ligne)*, la Cour a de même estimé que « l'insertion par Fashion ID du bouton "j'aime" de Facebook sur son site Internet lui permet d'optimiser la publicité pour ses produits en les rendant plus visibles sur le réseau social Facebook lorsqu'un visiteur de son site Internet clique sur ledit bouton. C'est afin de pouvoir bénéficier de cet avantage commercial consistant en une telle publicité accrue pour ses produits que Fashion ID, en insérant un tel bouton sur son site Internet, semble avoir consenti, à tout le moins implicitement, à la collecte et à la communication par transmission des données à caractère personnel des visiteurs de son site, ces opérations de traitement étant effectuées dans l'intérêt économique tant de Fashion ID que de Facebook Ireland, pour qui le fait de pouvoir disposer de ces données à ses propres fins commerciales constitue la contrepartie de l'avantage offert à Fashion ID… Dans de telles circonstances, il peut être considéré, sous réserve des vérifications auxquelles il incombe à la juridiction de renvoi de procéder, que Fashion ID et Facebook Ireland déterminent, conjointement, les finalités des opérations de collecte et de communication par transmission des données à caractère personnel en cause au principal » ; C.J., 29 juillet 2019, arrêt *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV*, C-40/17, points 80-81.

68 EDPB, Lignes directrices 8/2020 sur le ciblage des utilisateurs de médias sociaux, 13 avril 2021, en particulier p. 17.

69 C.J., 29 juillet 2019, arrêt *Fashion ID GmbH & Co. KG c. Verbraucherzentrale NRW eV*, C-40/17.

70 C.J., 5 juin 2018, arrêt *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH,* C-210/16.

71 La décision de l'APD du 22 février 2022 a fait l'objet d'un recours auprès de la Cour des marchés. La Cour belge, dans son arrêt du 7 septembre 2022, n° 2022/5760, (https://www.autoriteprotectiondonnees.be/publications/arret-provisoire-du-7-septembre-2022-de-la-cour-des-marches-ar-292-disponible-en-neerlandais.pdf) demande à la Cour de justice si la TC String créée dans le cadre du TCF peut être qualifiée de donnée personnelle à l'égard de IAB Europe et si IAB Europe peut être considérée comme responsable du traitement alors que cette société se présente comme une simple organisation sectorielle de normalisation, qui met à disposition de ses membres un cadre assurant la conformité de ses derniers au RGPD. Sur ces décisions et leur analyse, lire J. Eynard et M. Pradet, *op. cit. ;* M. Veale, M. Nouwens et C. Teixera Santos, « Impossible Asks : Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA ? », *Technology and Regulation*, 2022, pp. 12-22. Disponible sur https://doi.org/10.26116/techreg.2022.002.

nées du fait des traitements rendus possibles et propres à ces tiers[72] ? Il m'apparaît difficile de les rendre responsables « conjoints » de l'ensemble des traitements concrets générés par les utilisateurs clients de cette infrastructure[73]. Certes, la sécurité, la régulation et le contrôle de l'utilisation de cette infrastructure me semblent devoir faire l'objet d'une réglementation spécifique. Cette réglementation doit trouver à s'appliquer, outre l'application des règles du RGPD si le responsable de l'infrastructure est en même temps au titre cette fois de ses propres traitements, responsable du traitement[74] des données à caractère personnel dont le traitement ressort à la finalité même du fonctionnement de l'infrastructure[75].

19. À propos toujours de la réglementation des acteurs cumulant leurs propres données et celles obtenues dans le cadre des services d'infrastructure, on ajoute les dispositions européennes récentes prises à propos des infrastructures des « gatekeepers » pour lesquelles une réglementation spécifique limitant l'utilisation des données obtenues dans le cadre des services offerts aux utilisateurs de ces plateformes. Le Digital Market Act les soumet à des obligations supplémentaires au vu de leur rôle de « gatekeepers » (contrôleurs d'accès) : « Tout contrôleur d'accès est tenu de ne pas : a) traiter, aux fins de la fourniture de services de publicité en ligne, les données à caractère personnel des utilisateurs finaux qui recourent à des services de tiers utilisant des services de plateforme essentiels fournis par le contrôleur d'accès ; b) combiner les données à caractère personnel provenant du service de plateforme essentiel concerné avec les données à caractère personnel provenant de tout autre service de plateforme essentiel ou de tout autre service fourni par le contrôleur d'accès, ni avec des données à caractère personnel provenant de services tiers ; c) utiliser de manière croisée les données à caractère personnel provenant du service de plateforme essentiel concerné dans le cadre d'autres services fournis séparément par le contrôleur d'accès, y compris d'autres services de plateforme essentiels, et inversement ; et d) inscrire les utilisateurs finaux à d'autres services du contrôleur d'accès dans le but de combiner de données à caractère personnel, à moins que ce choix précis ait été présenté à l'utilisateur final et que ce dernier ait donné son consentement au sens de l'article 4, point 11), et de l'article 7 du règlement

72 Comme c'est le cas dans les affaires *IAB*, *Fashion ID* et *Wirtschaftsakademie*, précitées.

73 Par contre, le fait qu'il y ait communauté d'intérêts entre une « maison mère » et ses « filiales », intérêts poursuivis certes par des rôles différents assignés à l'un et l'autre nous paraît devoir conduire à la qualification de responsables conjoints. Il est à noter que les décisions citées ont été justifiées par la volonté de donner un effet utile aux dispositions du RGPD en faveur de la protection des personnes concernées. On peut accepter cet élargissement mais il nous apparaît inadéquat dans la mesure où une exacte qualification légale des responsables d'infrastructure permettrait à l'avenir une meilleure protection de ces personnes. Voy. C.J., 13 mai 2014, arrêt *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*, C-131/12 ; C.J., 10 juillet 2018, arrêt « *Témoins de Jéhovah* », C-25/17.

74 À cet égard, l'article 3.1 du Data Act proposé par la Commission prévoit à propos des produits IoT : « La conception et la fabrication des produits, et la fourniture des services liés, sont telles que les données générées par leur utilisation sont, par défaut, facilement, de manière sécurisée et, lorsque cela est pertinent et approprié, directement accessibles à l'utilisateur ».

75 Ce qui était le cas en ce qui concerne la décision *IAB* précitée. En effet, IAB se réservait le droit d'accéder aux données détenues par ses clients à des fins de contrôle du respect du TCF (*Transparency and Consent Framework*) qui régissait les conditions d'utilisation des données par les clients de IAB. On note cependant que dans l'affaire *Wirtschaftsakademie*, la Cour estime : « En tout état de cause, la directive 95/46 n'exige pas, lorsqu'il y a une responsabilité conjointe de plusieurs opérateurs pour un même traitement, que chacun ait accès aux données à caractère personnel concernées » ; C.J., 5 juin 2018, arrêt *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, point 38.

(UE) 2016/679. Lorsque le consentement donné aux fins du premier alinéa a été refusé ou retiré par l'utilisateur final, le contrôleur d'accès ne réitère pas sa demande de consentement pour la même finalité plus d'une fois par période d'un an »[76]. La proposition de Data Act contient de même des dispositions qui protègent l'utilisateur final et donc les personnes concernées en interdisant aux « gatekeepers » d'être destinataires des données collectées via le système d'IoT[77]. Ne peut-on considérer que certaines obligations voire interdictions pourraient être imposées à de telles entreprises en matière de protection des données à caractère personnel avec comme fondement : le service universel[78] rendu par ces plateformes, essentiel à la vie de toute personne dans notre société du numérique ? À cet égard, on évoquera, de manière analogique, le précédent des dispositions de la directive « *e-Privacy* » à propos des opérateurs de service de communication et limitant de manière sévère les traitements opérés par ces derniers[79].

[76] Article 5.2 du DMA.

[77] Voy. l'article 5.2 : « Toute entreprise fournissant des services de plateforme essentiels dont un ou plusieurs ont été désignés comme contrôleur d'accès […] n'est pas un tiers éligible au titre du présent article et ne peut par conséquent pas : (a) inviter un utilisateur, par une sollicitation ou par une incitation commerciale, quelles qu'elles soient, y compris en fournissant une compensation pécuniaire ou de toute autre nature, à mettre à la disposition de l'un de ses services des données que l'utilisateur a obtenues à la suite d'une demande introduite au titre de l'article 4, paragraphe 1, (b) inviter un utilisateur, par une sollicitation ou par une incitation commerciale, à demander au détenteur de données de mettre des données à la disposition de l'un de ses services conformément au paragraphe 1 du présent article, (c) recevoir d'un utilisateur des données que ce dernier a obtenues à la suite d'une demande introduite au titre de l'article 4, paragraphe 1 ».

[78] Comparer la notion de « service essentiel » reprise par le DMA, en particulier dans les considérants 13 et s. ; « C'est le cas en particulier pour les services numériques répandus et couramment utilisés, qui servent, pour la plupart, d'intermédiaires directs entre les entreprises utilisatrices et les utilisateurs finaux, et qui se caractérisent principalement par des économies d'échelle extrêmes, des effets de réseau très importants, la capacité de relier de nombreuses entreprises utilisatrices avec de nombreux utilisateurs finaux grâce au caractère multiface de ces services, des effets de verrouillage, l'absence de multi-hébergement ou l'intégration verticale. Il n'existe souvent qu'une seule grande entreprise ou très peu de grandes entreprises fournissant ces services numériques. Le plus souvent, ces entreprises sont devenues des contrôleurs d'accès pour les entreprises utilisatrices et les utilisateurs finaux, avec de profondes répercussions. En particulier, elles ont acquis la capacité de fixer facilement des conditions générales commerciales de manière unilatérale et préjudiciable pour leurs entreprises utilisatrices et utilisateurs finaux. Par conséquent, il est nécessaire de se concentrer uniquement sur les services numériques les plus largement utilisés par les entreprises utilisatrices et les utilisateurs finaux et pour lesquels les préoccupations relatives à la faible contestabilité et aux pratiques déloyales des contrôleurs d'accès sont plus apparentes et urgentes du point de vue du marché intérieur ».
Le considérant 14 indique que : « En particulier, les services d'intermédiation en ligne, les moteurs de recherche en ligne, les systèmes d'exploitation, les réseaux sociaux en ligne, les services de plateformes de partage de vidéos, les services de communications interpersonnelles non fondés sur la numérotation, les services d'informatique en nuage, les assistants virtuels, les navigateurs internet et les services de publicité en ligne, y compris les services d'intermédiation publicitaire, sont tous capables de toucher un grand nombre d'utilisateurs finaux comme d'entreprises, ce qui comporte un risque de pratiques commerciales déloyales. Ils devraient donc être inclus dans la définition des services de plateforme essentiels et relever du champ d'application du présent règlement ».

[79] Voy. l'article 6.5 de la directive vie privée et communications électroniques précitée (modifiée depuis en 2009 et en cours de révision par un règlement) : « Le traitement des données relatives au trafic, conformément aux paragraphes 1, 2, 3 et 4, doit être limité aux personnes agissant sous l'autorité des fournisseurs de réseaux de communications publics et de services de communications électroniques accessibles au public qui gèrent la facturation ou la gestion du trafic, les demandes de renseignements des clients, la détection des fraudes, la commercialisation de services de communications électroniques ou la fourniture d'un service à valeur ajoutée, et doit être limité à ce qui est nécessaire aux fins de ces activités ».

V. L'APPROCHE INDIVIDUALISTE DU RGPD – UNE LACUNE IMPORTANTE À L'HEURE DE NOTRE SOCIÉTÉ NUMÉRIQUE

20. Ce dernier point de notre réflexion critique l'approche suivie par nos réglementations de protection des données, à savoir celle individualiste qui n'entend protéger nos libertés qu'à travers le prisme de la défense des intérêts des personnes physiques. Cette approche a pour conséquence d'abandonner à la personne concernée le soin de sa propre protection. Notre propos suit donc deux temps : le premier analyse le rôle du consentement dans l'économie de la protection des données, rôle qui tend à affirmer une conception qualifiée de « propriétaire » des données à caractère personnel[80]. Dans un second temps, nous montrerons combien cette approche individualiste est de plus en plus partielle au regard des risques collectifs, sociétaux voire « systémiques », comme les qualifie le récent DSA, et nous redéfinirons le rôle de nos législations et de nos autorités dans le cadre de cet élargissement des préoccupations qu'engendre notre société du numérique.

A. La remise en cause du consentement, comme première cause de licéité des traitements

21. Avant d'entamer cet examen, notons que le consentement comme base de licéité des traitements n'a été affirmé explicitement qu'avec la directive de 1995[81]. Les premiers textes n'en font pas mention et, sans doute, sont-ce les attendus célèbres de l'arrêt de la Cour constitutionnelle allemande du 15 décembre 1983 à propos du recensement statistique rappelé ci-dessus[82], consacrant le principe d'autodétermination informationnelle qui expliquent cette insertion. La directive prend soin d'exiger un consentement libre, informé et spécifique[83] ; le RGPD ajoute que la manifestation de volonté doit être univoque, que le consentement est rétractable et ne peut être une condition « superflue » de l'exécution d'un contrat[84]. 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[85] ou le statut « vulnérables » de certaines personnes concernées[86] rendent invalide le consentement. La complexité des montages des systèmes supportés par les technologies de l'IA, la diversité des sources utilisées, l'effet « domino », l'impossibilité de

80 À propos de cette approche « propriété-exclusion » de la donnée et de sa remise en cause profonde en Europe au profit d'une approche « droit de contrôle et droit d'accès » autour d'une donnée considérée comme une « commons » au sens d'Ostrom, et ce à la faveur d'une politique volontariste de partage des données, lire mes développements « Data : from "Property" towards "Commons" », *Liber Amicorum Serge Gutwirth* (à paraître) et ceux de T. Tombal, *op. cit.*, pp. 55 et s.

81 Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 181/31, 23 novembre 1995 (ci-après « directive 95/46/CE »).

82 C. const. allemande, 15 décembre 1983, 1 BvR 209/83.

83 Article 2, sous h), de la directive 95/46/CE précitée.

84 Article 7 du RGPD.

85 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. À ce propos, voy. A. Gobert, note sous CNIL, décision du 29 décembre 2022, *R.D.T.I.*, 2023, pp. 144-158.

86 Ainsi, le travailleur, le candidat à un emploi ou le malade…

prévoir les corrélations qui seront à la base des décisions du responsable du traitement 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 pousse 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[87]. 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.

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 non la médiation des autorités de protection des données). Sans doute, faut-il, dans certains cas, interdire en principe le consentement[88] et réclamer que seules les autres causes de validité soient invocables[89], 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[90] ? Au-delà, il importe que

87 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), P9_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».

88 Ainsi, la loi du 4 avril 2014 prévoit en son article 46/2 que : «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». La loi belge poursuit en disposant que «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» (article 46/3) ; loi du 4 avril 2014 relative aux assurances, *M.B.*, 30 avril 2014, p. 35487. De manière plus nette encore, le «Genetic Information Nondiscrimination Act» (GINA) américain du 21 mai 2008 interdit l'utilisation de certaines catégories de données génétiques en matière d'emploi et d'assurance. On doit s'attendre à une multiplication de telles réglementations spécifiques vu les risques importants de discrimination en matière de santé, d'éducation, d'emploi et d'accès à des services financiers ou d'assurance que représentent les capacités prédictives et décisionnelles de l'IA.

89 À cet égard, voy. les réflexions de J. Eynard, *op. cit.*, p. 21 et de E. Deraedts, «À propos des dérives actuelles du consentement en matière de protection des données», *Actualités juridiques, Droit administratif*, n° 6, 2021, p. 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».

90 On reprendra volontiers sur ces deux points (droit à l'anonymat et droit à ne pas être profilé), la recommandation 3.6 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

la personne concernée puisse dans certains cas de traitements fondés sur des systèmes d'intelligence artificielle (en particulier lorsqu'il s'agit de traitements de profilage à des fins publicitaires[91]), définir la finalité du profilage qu'elle souhaite et, dès lors, réduire le champ des données qui seront exploitées.

22. De manière plus fondamentale, ne peut-on considérer que le consentement met la personne concernée au centre de la responsabilité de la protection de ses propres données en lui donnant, dans le même temps, l'illusion d'une « propriété » de ses données[92] alors même qu'il n'en est rien ? Par ailleurs, peut-on faire dépendre la légitimité d'un traitement sur 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[93] ? Sans doute, cette remarque renvoie à la dimension collective et sociétale du débat « vie privée », dimension qui, comme nous l'analysons maintenant, est obscurcie par la dimension purement individualiste de nos législations de protection des données.

qui était nécessaire à l'exécution de la prestation et ce après avoir été informée […] » ; Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, « Profilage et la Convention 108+ : pistes pour une actualisation », T-PD(2019)07BISrev, 7 novembre 2019.

91 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, par contre, 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…

92 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*, Paris, LexisNexis, 2022, pp. 75-117.

93 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 la base de l'article 6, f), du RGPD sans que pour autant ce ne soit nécessaire à l'exécution du contrat et pourrait porter atteinte à la dignité de la personne ?

B. Vers un élargissement des préoccupations : le rôle essentiel mais partiel du RGPD et de nos autorités

23. Les discussions actuelles qui entourent les textes européens nouveaux encadrant l'économie des données élargissent nettement le débat. Ces textes entendent prendre en compte non seulement les risques encourus pour nos libertés individuelles ou mettant en péril nos intérêts de consommateur (voy. les systèmes de recommandation de biens ou produits) mais également les risques de discrimination et de non-respect des valeurs de justice sociale voire les risques sociétaux, comme les questions environnementales, les atteintes à l'État de droit et à la démocratie[94]. Ainsi, la proposition IA Act[95] entend élargir le champ de l'évaluation au regard de celui auquel le RGPD se limitait. Selon le texte de la proposition, elle complète les règlements déjà existants (le RGPD, mais également d'autres actes comme celui sur la non-discrimination, l'égalité des genres, la sécurité, la protection des consommateurs, etc.) « avec un ensemble de règles harmonisées concernant la conception, le développement et l'utilisation de certains systèmes d'IA à haut risque ainsi que des restrictions portant sur certaines utilisations de systèmes d'identification biométrique à distance… »[96].

L'« ethical values assessment » proposé dans le cadre du projet de règlement IA[97] déborde dès

94 Sur la prise en compte de ces trois catégories de risques présentes dans les textes internationaux en matière d'éthique de l'IA, lire Y. Poullet, « About some international documents relating to the ethics of Artificial Intelligence – Some insights », in H. Jacquemin (dir.), *Time to reshape the Digital Society*, Actes du 40e anniversaire du CRIDS, coll. Cahiers du CRIDS, no 52, Bruxelles, Larcier, 2021, pp. 501 et s.

95 Ainsi, lorsqu'il est fait référence aux « droits fondamentaux » mis en cause par l'IA et que la proposition vise à protéger, le point 3.5 de l'exposé des motifs souligne que : « L'utilisation de l'IA, compte tenu des caractéristiques spécifiques de cette technologie (par exemple l'opacité, la complexité, la dépendance à l'égard des données, le comportement autonome), peut porter atteinte à un certain nombre de droits fondamentaux consacrés dans la Charte des droits fondamentaux de l'UE (ci-après la "Charte"). La présente proposition vise à garantir un niveau élevé de protection de ces droits fondamentaux et à lutter contre diverses sources de risques grâce à une approche fondée sur les risques clairement définie. Prévoyant un ensemble d'exigences pour une IA digne de confiance et des obligations proportionnées pour tous les participants à la chaîne de valeur, la proposition renforcera et favorisera la protection des droits protégés par la charte : le droit à la dignité humaine (article 1er), le respect de la vie privée et la protection des données à caractère personnel (articles 7 et 8), la non-discrimination (article 21) et l'égalité entre les femmes et les hommes (article 23). Elle vise à prévenir un effet dissuasif sur les droits à la liberté d'expression (article 11) et à la liberté de réunion (article 12), à préserver le droit à un recours effectif et à accéder à un tribunal impartial, les droits de la défense et la présomption d'innocence (articles 47 et 48), ainsi que le principe général de bonne administration. En outre, la proposition renforcera les droits d'un certain nombre de groupes particuliers dans différents domaines d'intervention, notamment les droits des travailleurs à des conditions de travail justes et équitables (article 31), le droit des consommateurs à un niveau élevé de protection (article 28), les droits de l'enfant (article 24) et l'intégration des personnes handicapées (article 26). Le droit à un niveau élevé de protection de l'environnement et l'amélioration de la qualité de l'environnement (article 37) sont également pertinents, y compris au regard de la santé et de la sécurité des personnes. Les obligations relatives aux essais *ex ante*, à la gestion des risques et au contrôle humain faciliteront également le respect d'autres droits fondamentaux en réduisant au minimum le risque de décisions erronées ou biaisées assistées par l'IA dans des domaines cruciaux tels que l'éducation et la formation, l'emploi, les services essentiels et l'appareil répressif et judiciaire ».

96 Voy. le point 1.2 de l'exposé des motifs de la proposition AI Act.

97 Sur ce point, voy. les travaux du Groupe d'experts de haut niveau sur l'intelligence artificielle de la Commission. Sur ce groupe et ses travaux, voy. https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence. Ces travaux avaient abouti, en avril 2019, à la publication de lignes directrices éthiques pour une IA digne de confiance (texte disponible sur le site : https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-

lors de celui imposé par le *Privacy Impact Assessment* mis en place par le RGPD et s'indique lorsqu'il s'agit de traitements de données à caractère personnel utilisant des systèmes d'IA. Trois commentaires à ce sujet : le premier est l'ampleur du travail[98] et des compétences à réunir ou à coordonner lorsqu'il s'agira de procéder à l'occasion, par exemple, de l'évaluation d'applications destinées au pilotage de voitures intelligentes, à la confrontation des préoccupations de protection des données, de consommateurs, d'environnement et de non-discrimination ; le deuxième est le rôle du PIA, au sein de cette évaluation globale, est-il à mener distinctement et transmis ensuite au rapport souhaité par la proposition réglementaire ; troisièmement, on sait que le CEPD[99] a réclamé que les autorités de protection des données constituent les futures autorités de notification, en justifiant de leur compétence et de leurs expériences en matière de PIA. Or l'élargissement des préoccupations prises en compte par ces textes, et en particulier l'AI Act dont nous avons parlé, infirme cette prétention[100] : il est certain que d'autres organismes, tels les centres pour l'égalité des chances, les autorités en charge de la liberté d'expression, les organismes de protection des consommateurs… doivent également jouer un rôle au vu d'un tel élargissement… avec le risque évident de tensions voire de contradictions entre ces avis[101]. Dans une affaire allemande récente dans laquelle l'organisme en charge de veiller à la concurrence était partie, la Cour de justice de l'Union européenne[102] a ainsi considéré qu'il était nécessaire sur les questions de protection des données inhérentes à l'affaire que cet organisme défère de telles questions à l'autorité allemande de protection des données. Cette décision augure d'une répartition de responsabilités entre autorités administratives indépendantes et surtout de la nécessité de leur collaboration. Quoi qu'il en soit, la néces-

trustworthy-ai) et plus récemment à la publication d'une liste reprenant les critères d'évaluation des sept caractéristiques d'un AI digne de confiance (ALTAI ou *Assessment List for Trustworthy AI,* disponible sur : https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment). Les sept critères dégagés par les *guidelines* sont respectivement : Human Agency and Oversight ; Technical Robustness and Safety ; Privacy and Data Governance ; Transparency ; Diversity, Non-discrimination and Fairness ; Societal and Environmental Well-being ; Accountability.

98 À cet égard, on reste dubitatif sur la possibilité d'envisager l'ensemble des risques au vu du nombre des dispositions contenues dans la Charte européenne des droits fondamentaux.

99 Avis conjoint 05/2021 de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle, 18 juin 2021, disponible sur : https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_fr.pdf, en particulier la note 52.

100 Cela dit, il est légitime de reconnaître au regard des risques majeurs d'atteinte à la protection des données, encourus du fait de l'utilisation des systèmes d'IA et de leur particularité tant de prédiction, de profilage que l'opacité de fonctionnement, une certaine priorité à cette protection et la présence d'un membre de la CEPD dans le Comité européen de l'intelligence artificielle (articles 56 et s. de l'AI Act) qui coiffe l'ensemble des organismes nationaux de contrôle et de surveillance.

101 Prenons l'hypothèse d'un système d'IA permettant le calcul des primes d'assurance vie ou de véhicule au plus près des risques liés à chaque assuré. Ce système pourrait notamment avec la garantie du consentement éclairé individuel être jugé comme conforme aux exigences du RGPD et, par contre jugé discriminatoire par un organisme chargé de lutter contre la discrimination, au motif que la réduction des primes obtenue par les personnes jugées bons élèves entraîne un surcoût disproportionné pour d'autres et se révèle contraire au principe de mutualisation des risques.

102 C.J., arrêt *Meta vs. The German Bundeskartellamt*, C-252/21 (non encore publiée). L'avocat général dans son opinion déjà publiée considère que les autorités de la concurrence, au cas où l'examen du cas implique des questions de protection des données, doivent se référer à l'APD pour l'examen de cette partie du dossier ; av. gén., concl. préc., C.J., 20 septembre 2022, arrêt *Meta vs. The German Bundeskartellamt*, C-252/21.

sité d'une approche transversale, proposée par la Commission à propos des systèmes d'IA, ne peut, à notre avis, aboutir que par une clarification du rôle et des compétences de chaque catégorie d'autorités administratives[103] mais, surtout, par la création institutionnalisée de lieux de dialogue entre ces différents organes, sans quoi on risque des interventions dans des sens contradictoires voire des rivalités contre-productives entre instances.

24. À l'instar du texte relatif à l'intelligence artificielle, on relève que le même souci habite les autres textes récents déjà cités. Le Data Governance Act entend permettre un meilleur partage des données à la fois par une réutilisation plus importante des données détenues par des organismes du secteur public[104], et par un encadrement de la fourniture de services de partage des données[105] et en fixant un cadre pour les entités qui collectent et traitent les données mises à disposition du secteur public à des fins altruistes[106]. Le Data Act part de la même préoccupation : encourager le partage des données collectées dans le cadre de fonctionnement de systèmes basés sur l'internet des objets[107]. Dans ces différents textes, la donnée apparaît comme au confluent de droits différents aux titulaires aux intérêts souvent antagonistes que les textes cités cherchent à concilier. La donnée n'est plus la propriété de personne mais apparaît comme un « commun », au sens donné par Ostrom[108]. Le droit à la protection des données doit se concilier, tantôt se heurter, tantôt se conforter par sa rencontre avec le droit de la concurrence, le droit de la consommation, le droit de la propriété intellectuelle, le droit à la non-discrimination, le droit à la liberté d'expression, etc.

25. Abordons le dernier point mais non le moindre, la question des NBIC[109] et la place à donner à la protection des données en la matière. Les applications liées à la combinaison des technologies nano, bio, informatique, sciences cognitives donnent le vertige. On en cite deux. Le projet transhumaniste Neuralink d'E. Musk entend connecter, grâce à des implants placés dans le cortex, nos cerveaux à des ordinateurs capables d'améliorer nos capacités de mémoire, de calcul, de raisonnement voire nos émotions. La possibilité de modification ciblée de notre génome est désormais possible grâce à l'utilisation de ciseaux moléculaires qui, suivant la technologie CRISPR-Cas9[110], permet d'enlever de remplacer une partie défectueuse de l'ADN ou,

103 … et le renvoi par chaque autorité à l'autorité spécialisée lorsque l'examen d'une des questions soumises à sa compétence concerne cette autre autorité. Ainsi, dans l'arrêt, l'autorité de concurrence saisie de la question de la conformité d'une entente au droit de la concurrence s'est inquiétée de l'impact de l'entente entre entreprises sur le droit des personnes concernées à la protection de leurs données. La Cour a souhaité que ce point soit confié à l'analyse par l'autorité de protection ces données.

104 Articles 3-9 du DGA.

105 Articles 10-15 du DGA.

106 Articles 16 et s. du DGA.

107 Voy. le chapitre 2 du Data Act.

108 E. Ostrom, *La gouvernance des biens communs : pour une nouvelle approche des ressources naturelles*, Bruxelles, De Boeck, 2010. Voy. égal. E. Schlager et E. Ostrom, « Property rights and natural ressources : A conceptual analysis », *Law and Economics,* vol. 68, 1992, pp. 249-269 ; E. Ostrom et C. Hess, « Private and Common Property Rights » – *Workshop in Political Theory and Policy Analysis, Indiana University,* Research Paper No. 2008-11-01, disponible sur : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1936062.

109 Une science combinant les nanotechnologies (N), biotechnologies (B), informatique (I) et sciences cognitives (C).

110 Sur cette technologie et son application au cas chinois de modification sur des nouveau-nés de leur bagage génétique afin d'éviter la transmission de gênes des parents sidaïques, lire Comité d'éthique de l'INSERM, Saisine concernant les questions liées au développement de la technologie CRISPR *(clustered regularly interspaced short palindromic repeat)*-Cas9, inserm-02110670, 2016, disponible sur le site : https://www.hal.inserm.fr/inserm-02110670.

plus généralement, de modifier notre bagage génétique. Ces développements touchent à la notion de notre identité en tant qu'humain[111] et méritent, selon un devoir de précaution, une extrême prudence avant d'accepter de telles innovations, comme le prescrit, sur base de la Déclaration universelle de l'Unesco sur la bioéthique et les droits de l'homme l'UNESCO[112], l'article 16-4 du Code civil français « Nul ne peut porter atteinte à l'intégrité de l'espèce humaine. Toute pratique eugénique tendant à l'organisation de la sélection des personnes est interdite. Est interdite toute intervention ayant pour but de faire naître un enfant génétiquement identique à une autre personne, vivante ou décédée. Sans préjudice des recherches tendant à la prévention et au traitement des maladies génétiques, aucune transmission ne peut être apportée aux caractères génétiques dans le but de modifier la descendance de la personne ».

Dans ces débats, quels rôles pour la protection des données et leurs autorités ? Certes, on peut imaginer diverses interventions : celles de rappeler la nécessité de consentement mais n'est-il pas acquis lorsqu'aux *happy few* qui auront les moyens financiers d'avoir accès aux bénéfices de ces technologies, on fera miroiter les bénéfices de ces technologies pour eux ou pour leurs enfants ? Les autorités rappelleront, sans doute, que ces développements autorisés dans le cadre de la recherche médicale ou l'octroi de soins ne peuvent servir à des développements commerciaux destinés au bien-être de certains individus[113]. On ajoutera le devoir de PIA et de celui d'assurer la confidentialité des données ainsi obtenues. Toutes ces questions permettront certes une intervention mais celles-ci ne ratent-elles pas l'ambition qui avait été celle des premiers textes en matière de vie privée ? On rappellera l'article 1 de la loi informatique et libertés de 1978, malheureusement oublié lors de la rédaction du RGPD : « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». N'est-ce pas le devoir de nos autorités de dépasser le cadre étroit de la protection de nos données mais de rejoindre celui plus large de la vie privée définie, ainsi que l'affirme la jurisprudence du Conseil de l'Europe[114], comme fixant l'ensemble des conditions nécessaires à l'épanouissement de nos personnalités dans une société donnée. Dans une telle conception, l'exigence de vie privée ne se fonde pas sur

111 Parmi de nombreuses réflexions, lire E. Fourneret, *Le cerveau implanté. Penser l'homme à l'ère des implants cérébraux*, Paris, Hermann, 2022.

112 UNESCO, Déclaration universelle sur la bioéthique et les droits de l'homme, 19 octobre 2005.

113 Sans doute, est-il urgent de distinguer, même si la frontière semble de plus en plus floue, l'intervention sur le génome à des fins médicales, c'est-à-dire de soin réparateur (éthique du *care*), de celle qui se fonderait sur l'argument du bien-être de la personne (homme augmenté) ou, lorsque le traitement est pratiqué sur l'embryon, justifié par la volonté des parents voire l'amélioration de la race. En ce qui concerne la recherche médicale, peut-on accepter ou faut-il interdire l'édition du génome d'un embryon au nom de l'intérêt des générations futures ou plus pragmatiquement de l'intérêt thérapeutique qu'il pourrait apporter du fait des résultats de la recherche ? Sur toutes ces questions, lire l'ouvrage d'E. Fourneret, *op. cit.* On ajoute que le RGPD définit, en son article 4.15, la notion de données de santé comme révélant une information sur l'état de santé et dès lors pose des problèmes lorsqu'il s'agit de données de « bien-être », comme les données générées par des outils de mesure de soi ou les données recueillies dans le cadre d'un implant corporel pour limiter le stress d'un individu.

114 Sur l'analyse de la jurisprudence de la Cour de Strasbourg, la conception large qui s'en dégage et l'analyse de la réglementation de protection des données comme simple instrument au service de la vie privée et à interpréter en fonction de celle-ci, lire notre ouvrage et les références y citées, *La vie privée à l'heure de la société du numérique – Essai*, coll. Cahiers du CRIDS, n° 45, Bruxelles, Larcier, 2019.

le présupposé d'un individu capable *a priori* d'une maîtrise de son environnement via son consentement ou par l'exercice de ces droits, mais sur un État qui, dans un contexte sociétal donné, doit permettre, y compris par son intervention vis-à-vis des acteurs privés, l'épanouissement des personnes comme acteurs sociaux de changement.

26. Cette intervention doit tendre à assurer le respect d'un équilibre entre deux mouvements en tension et dont la synthèse caractérise bien le développement humain et auxquels renvoie, selon la jurisprudence du Conseil de l'Europe, le concept large de vie privée que la Charte de l'Union européenne a malheureusement dissocié en distinguant le respect de la vie privée et familiale de l'article 7, du droit à la protection des données à caractère personnel consacré par l'article 8. En effet, le même concept de vie privée justifie d'une part l'approche négative du concept : le droit à l'intimité et d'autre part, celle plus positive : le droit de maîtriser la circulation de son image informationnelle. D'une part, il s'agit de consacrer la nécessité de pouvoir se retirer et se mettre à l'abri du regard d'autrui et de sa surveillance : « The right to be let alone »[115] dont on conviendra qu'il est de plus en plus menacé, alors que les murs de nos maisons ne nous mettent plus à l'abri des surveillances nombreuses que nos ordinateurs, *smartphones* et autres instruments d'intelligence ambiante autorisent en permanence. Le droit de se déconnecter ou de communiquer anonymement mériterait une meilleure affirmation dans nos sociétés de surveillance et de présence ubiquitaire des outils de collecte des données. D'autre part, parce que l'Homme est un être social et que l'internet donne l'opportunité d'une société inclusive (problème de la justice sociale et de la discrimination), il s'agit de garantir les conditions de la confiance nécessaire à une coopération et une interaction entre les internautes, de libérer la parole de chacun tout en évitant les biais et les ruses, caractéristiques d'une société de contrôle et de maintenir l'identité humaine (problème du transhumanisme). Ce rétrécissement de la compétence de nos autorités de protection des données aux seules questions de protection des données nous apparaît dommageable, à l'heure où les technologies nouvelles du numérique « révolutionnent » nos sociétés et exigerait, me semble-t-il, un élargissement des réflexions de nos autorités redevenues « chiens de garde » au service de notre dignité, de notre identité et de nos libertés, condition de la vie de nos démocraties.

CONCLUSIONS

27. Que retenir de ces considérations volontairement critiques tant d'une réglementation que des acteurs chargés de la faire vivre ? Il est évident que loin de nous l'idée de contester tout l'apport du RGPD à la cause de nos libertés en Europe voire au-delà. Il est gigantesque. Le RGPD a induit une culture de la vie privée et l'intérêt chez chaque citoyen de mieux maîtriser son environnement informationnel. Notre propos n'est pas de condamner le texte mais d'en adoucir les angles pour certains acteurs, de les renforcer pour d'autres ; sans doute, d'avoir une approche plus proportionnée aux risques liés à certaines technologies ou infrastructures et, en tout cas, fruit de l'omnipotence de ces fameux « gatekeepers » de services devenus d'intérêt public. Au-delà, nous plaidons pour la création d'une autorité européenne ayant y compris une compétence juridictionnelle, au-delà des APD nationales.

Notre propos, en privilégiant l'approche par les risques, n'entend pas remettre en cause la multiplication des droits subjectifs progressi-

[115] « Le droit d'être laissé seul ».

vement consacrés par les différentes générations de réglementation vie privée mais l'exercice de ces droits subjectifs s'opère *a posteriori* de manière aléatoire et entraîne des procédures longues et aux résultats imprévisibles, à l'inverse de l'approche préventive d'évaluation interne voire externe des risques, évaluation multidisciplinaire et « multistakeholders » sur le modèle préconisé par la proposition d'AI Act.

28. La remise en cause du concept de données à caractère personnel, l'approche de la sensibilité des données, la nécessité de prendre en compte et donc de réglementer des acteurs difficilement qualifiables de responsables de traitement ou de sous-traitants s'imposent si on entend protéger effectivement les personnes concernées. Par ailleurs, à l'heure des technologies émergentes, une réflexion sur l'adéquation du texte s'avère nécessaire. Ne faut-il pas voir dans un certain nombre de textes européens récents une volonté de compléter le RGPD eu égard aux questions nouvelles posées par ces technologies ? Le souhait de voir remis en cause de manière plus nette encore l'approche individualiste propriétaire que nombre d'auteurs ont cru voir dans les dispositions assurant la prééminence du consentement a été exprimé nettement : face au déséquilibre informationnel croissant entre, d'une part, l'utilisateur des applications technologiques, qu'il soit personne physique ou morale et, d'autre part, ceux qui disposent de l'information et de moyens toujours plus importants de la traiter de manière « utile », il est illusoire de confier à la seule personne concernée sa défense.

Dans cette même ligne de réflexion, regrettons la décision de la Charte des droits fondamentaux de l'Union européenne de séparer en les consacrant par deux articles distincts (articles 7 et 8) le respect de la vie privée et familiale et la protection des données à caractère personnel. Cette distinction va à l'encontre de l'idée même de vie privée, telle que définie et interprétée par le Conseil de l'Europe comme garantie de la possibilité pour chacun de développer sa personnalité, ce qui implique à la fois le droit négatif de ne pas participer à la société de l'information (soit le droit d'être laissé seul) et celui plus positif, en cas de participation, de pouvoir maîtriser son environnement informationnel. Regrettons qu'à l'heure de l'ubiquité du numérique, le premier aspect largement consacré dans les premières législations ne soit pas mieux développé et consacré explicitement au-delà du droit à l'oubli comme droit de ne pas être surveillé et de pouvoir échapper aux connexions opérées à son insu et en toute hypothèse pouvoir les bloquer facilement.

29. Enfin, on s'interroge sur la possibilité pour nos autorités tout occupées par les méandres des textes et des procédures et réduite à la compétence de la protection de nos données de pouvoir s'attaquer aux questions fondamentales que le développement inquiétant du numérique pose au-delà de nos libertés, à notre identité, à notre société qui pourtant naissent des développements du numérique sans qu'elle se donne comme grille de lecture, les valeurs de dignité et d'épanouissement de la personnalité, éléments fondateurs du concept de vie privée. L'effacement progressif de la délibération politique par une « gouvernementalité algorithmique », selon l'expression chère à A. Rouvroy[116], la normalisation des comportements par une régulation technologique insidieuse et ubiquitaire, la prise en compte de plus en plus exclusive de la donnée par rapport au récit et à la rencontre des personnes, les manipulations génétiques et les technologies au service de l'homme augmenté exigent une réflexion plus globale que celle proposée par les législations

[116] A. Rouvroy et T. Berns, « Gouvernementalité algorithmique et perspectives d'émancipation – Le disparate comme condition d'individuation par la relation ? », *Réseaux,* 2013/1, n° 177, pp. 163-196.

de protection des données. Que nos autorités de protection des données s'aventurent comme elles commencent déjà à le faire dans ces débats est certes important mais surtout qu'elles ne confisquent pas le débat. Qu'elles le fassent en pleine synergie avec les autres autorités indépendantes en charge de l'égalité des chances, de protection des consommateurs, de concurrence, de liberté d'expression, qu'elles se concertent avec les comités d'éthique des sciences, de bioéthique ; qu'ensemble, ces autorités participent à une évaluation de nos technologies du numérique, est indispensable. Qu'elles n'hésitent pas chacune dans leur domaine ou ensemble à porter le débat devant le public et les organes de nos démocraties, chaque fois que l'enjeu sociétal le nécessite.