Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Cinq ans après

Poullet, Yves

Published in:
Revue des affaires européennes

Publication date:
2021

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 2021, 'Cinq ans après: le RGPD et les défis du profilage à l'heure de l'intelligence artificielle', *Revue des affaires européennes*, numéro 1, pp. 87-101.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 02. May. 2026

Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle*

Five years on: the GDPR and the challenges of profiling in the age of artificial intelligence

Yves POULLET, *Professeur émérite à la Faculté de droit de Namur, Professeur associé à l'UCLille, Membre de l'Académie royale de Belgique*

« *Nous voulons que l'application de ces nouvelles technologies soit digne de la confiance de nos citoyens [...] Nous encourageons une approche responsable de l'intelligence artificielle centrée sur l'humain* »
(Déclaration d'U. VAN DER LEYEN,
Présidente de la Commission lors de l'annonce
du plan stratégique de l'Union européenne
en matière d'intelligence artificielle,
le 19 février 2020).

Artificial intelligence – Bias – Opacity – Stakeholders – Infringement of individual and collective liberties – Merits and limits of the RGPD – Ethical approach

Profiling activities are developing in all spheres of activity. It might be the administration wishing to better track down offenders, including potential offenders, or to offer more adequate services to citizens.

It might be companies that want to know their current or future customers better, offer them new services or better select their employees; endly, it might be hospitals or medical scientific research institutes fighting against diseases or using the technologies for achieving better care. Today, different technologies: Internet of things, big data and artificial intelligence applied together are modifying radically the methods and the impact of profiling activities. AI systems often operate, with potential bias and errors,

* La présente contribution renvoie à des réflexions plus développées publiées par ailleurs. Cf. Y. POULLET, *Le RGPD face à l'intelligence artificielle*, Cahier du CRIDS, n° 49, Bruxelles, Larcier, 2020 et le rapport B. FRENAY – Y. POULLET, *Profiling and Convention 108+: Report on developments after the adoption of Recommendation (2010)13 on profiling*, rapport établi pour le Conseil consultatif de la Convention n° 108, novembre 2019 dans le cadre de la révision de la recommandation de 2010 sur le profilage, rapport à paraître. Le texte est à jour à la date du 10 mars 2021 et n'a dès lors pu tenir compte de textes parus depuis, en particulier de la « Proposal for a Regulation of the EU Parliament and of the Council laying down harmonised rules on artificial intelligence and amending certain Union legislative Acts », proposition émanant de la Commission européenne, Bruxelles, 21 avril 2021, COM(2021) 206 final.

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

in an opaque fashion combining the functioning of multiple neural networks. They rely on random statistical combinations taking into account millions of data items and now make possible unprecedented efficient and predictive profiling of individual behavior. That reality and the possible lack of human mastership of the technology increase the risks incurred individually by the data subjects but also collectively by groups of individuals and more essentially for our democracy and rule of law. Taking into account all, these elements, the GDPR does present certain shortcomings both as regards its definitions, its principles and overall as regards its scope.

These reasons militate in favor of a rethought and renewed regulatory framework for profiling and definitively open the way for an enlargement about ethical issues like discrimination, democracy and groups' privacy as requested by certain recent EU and Council of Europe initiatives.

1. Le phénomène du profilage n'est pas neuf. De tout temps, chacun de nous « profile » autrui. Nous cherchons tous à catégoriser ceux qui nous entourent à partir de leurs caractéristiques personnelles qu'elles soient pertinentes, objectives, permanentes ou non. Bref, nous utilisons les données subjectives ou objectives en notre possession pour catégoriser autrui et inférer, sans doute avec une marge d'erreur dans notre appréciation, d'autres traits ou manières d'être, qui nous sont inconnus. Le profilage est donc une opération propre à tout être humain, dans la mesure où nous cherchons tous à pouvoir nommer le réel qui nous entoure ou, en d'autres mots, à faire entrer autrui dans des catégories qui permettent de mieux le cerner et agir vis-à-vis de lui. Cependant, l'utilisation de systèmes d'information fondés sur l'IA modifie les modalités et la portée du profilage de manière essentielle et ce pour diverses raisons.

La première tient au fait que les systèmes d'information actuels par leur interactivité, leur interconnexion et leur ubiquité permettent d'élargir – et ce de manière exponentielle – le nombre de données collectées et traitées. Si hier, les capacités de stockage et de communication des données étaient limitées, aujourd'hui, d'une part, ces capacités sont devenues quasiment infinies comme le démontre le phénomène des méga-données (le *big data*) et, d'autre part, l'internet des objets connectés (en 2025, il est prévu que chaque citoyen européen rencontrera par jour plus de 4 800 objets). En outre, la multiplication des services disponibles à portée d'un clic permet la capture de moments de plus en plus triviaux de la vie quotidienne. Le numérique est désormais, partout dans nos poches, nos voitures, nos murs, nos vêtements, notre corps et nous révèle de manière continue, par morceaux, autant de pièces d'un puzzle que le détenteur de ces données pourra recomposer et ainsi « profiler » de manière de plus en plus fine et de plus en plus proche l'individu auquel ces données sont rapportées.

La seconde est l'utilisation d'algorithmes toujours plus puissants pour analyser cette quantité de données. Il y a vingt ans, les « profileurs » s'aidaient d'algorithmes fondés sur une mise en forme du raisonnement humain. Ces systèmes dits experts permettaient de se substituer (ou en tout cas d'aider) au travail du responsable de traitement dans la mesure où ces systèmes traduisent et appliquent automatiquement les « règles » causales et logiques mises en forme par des experts humains sur la base de leurs expériences. Ces systèmes d'IA dits symboliques guidaient ainsi le raisonnement du banquier lors de la délivrance d'un crédit, un assureur dans la fixation d'une prime ou un juge lors de l'octroi d'une pension alimentaire. Ces systèmes évitaient partiellement la subjectivité et les risques de discrimination propres à tout décideur humain. À ces systèmes experts dont l'algorithme est totalement transparent, succèdent aujourd'hui des systèmes dits de « *machine learning* », voire de *deep learning*, capables de travailler sur bien plus de données que celles traitables par les experts voire par un cerveau humain. Ces systèmes opèrent des corrélations entre des données de plus en plus nombreuses par des interactions entre réseaux de neurones de plus en plus puissants et ce, suivant des algorithmes qui se nourrissent et s'affinent progressivement au fur et à mesure des données rencontrées. La variété et

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

la complexité des « modèles » suivis et développés par ces algorithmes sont telles que leur fonctionnement purement statistique devient partiellement non transparent y compris pour ceux qui les ont développés et/ou les utilisent. La décision qu'ils prennent apparaît comme une « vérité », sortie de l'ordinateur sans transparence de sa motivation. Alors que les systèmes experts traditionnels travaillaient sur des profils auxquels ils faisaient correspondre des personnes, ici, dans les systèmes de profilage utilisant le *machine learning*, le profil n'est plus énoncé, il s'inscrit de manière non reconnaissable dans la décision prise par l'ordinateur suivant le modèle donné à son fonctionnement purement statistique et en tout cas partiellement opaque.

I. Le profilage et l'IA – Pourquoi ? quels risques[1] ?

2. Trois arguments expliquent le recours croissant de nos administrations et de nos entreprises à l'IA : le premier est certes l'optimisation : les systèmes IA permettent de maximiser la recherche du bon client, locataire ou du bon employé ; ils constituent un auxiliaire précieux tant dans la définition des stratégies de nos dirigeants (il suffit de voir l'utilisation de l'IA dans la lutte contre la COVID-19), que pour veiller à la bonne exécution des réglementations : ainsi détecter les potentiels fraudeurs ou les futurs délinquants. Nos médecins utilisent des robots pour analyser et comparer avec une précision infinie des images scannées et les laissent guider leurs interventions chirurgicales. Les systèmes IA garantissent une meilleure recherche médicale, parfois réalisée en dehors du monde médical. Ainsi, IBM révélait il y a peu que des systèmes de *deep learning* d'analyse de l'évolution du langage et du vocabulaire utilisé par un internaute dans des messages sur les réseaux sociaux, de la frappe sur le clavier de l'ordinateur et des recherches effectuées révélaient mieux que l'analyse médicale classique la présence précoce de la maladie d'Alzheimer. Autre déclaration, celle d'un directeur de recherche de Microsoft : désormais, affirme-t-il, « *nous pouvons prédire des événements non modélisables. Par exemple, Cornell University et nous détectons (mieux que le corps médical) la survenance de l'état dépressif de patients bipolaires en analysant les changements dans la frappe de messages sur l'écran d'un smartphone* ». On pointe également la création par Google de Calypso, un vaste centre de recherches sur le vieillissement qui travaille sur le transhumanisme. Que penser de cette irruption des entreprises du TECH dans le domaine de la santé, traditionnellement protégé par la déontologie des praticiens de l'art de guérir ? Pour quelles finalités ? Avec quels destinataires ?

Au-delà, toujours en ce qui concerne l'optimisation, ne peut-on considérer que le *droit invite* à l'utilisation de systèmes IA, lorsque, par exemple, il demande au banquier de mieux connaître son client ou à la plateforme YouTube ou Google Search de lutter contre la copie illicite ? Pour répondre à cette invitation, quoi de mieux que l'utilisation de systèmes IA ? Au-delà, la tentation est forte pour le *droit de déléguer* à la machine le soin de veiller à son exécution voire avec la justice prédictive, le soin de trancher à la place de nos magistrats. Ne serait-ce pas plus rapide, efficace et en définitive juste ?

3. La sécurisation est un deuxième argument. Sécurisation dans la lutte contre le danger du terrorisme (l'Europe met au point un système d'IA capable à partir de questionnaires, de reconnaissance faciale, d'interrogation de bases de données, de repérer parmi les immigrants se précipitant à nos frontières, les « terroristes » d'hier ou de demain) ; sécurisation dans l'utilisation de l'IA pour détecter des mouvements suspects dans un aéroport ou des chutes de personnes âgées dans des EPAHDs ; sécurisation dans la détection et la réaction à des malwares ; …

L'objectivation est sans doute le dernier argument mais il n'est pas le moindre. Le fonctionnement d'une machine neutre travaillant sur des données qui ne mentent pas elles (ce qui laisse supposer par ailleurs que les personnes elles mentent) est un excellent argument contre celui qui prétendrait que votre décision est subjective. Au sein des entrepôts de données, les individus sont approchés non plus en tant que personnes mais à travers, d'une part, l'agrégation d'un certain nombre de données les concernant, considérées d'autant plus comme « vérité » de chacun de nous qu'elles représentent des instantanés

[1] Sur tous ces points, nous recommandons la lecture de l'essai de Y. Meneteu, *L'intelligence artificielle en procès*, coll. Micro Droit. Macro Droit, Bruxelles, Bruylant, 2020.

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

de vie (ma présence à tel endroit, mon *surfing*, mes heures et mes « objets » d'écoute, mon achat de tel produit, ma consommation d'énergie) et, d'autre part, la mise en corrélation de telles données avec des données de même type collectées auprès d'autres individus ou des données anonymes propres à des entités ou groupes auxquels j'appartiens. À la vérité des données saisies sur le vif, s'ajoute celle que confère la statistique. Comment nier que telle personne puisse être fraudeuse, le candidat idéal ou la personne intéressée par telle publicité ou tel parti politique puisque son « profil » ou plutôt le « modèle » démontre que 95 % des personnes ayant le même profil révèlent cette même capacité ou ce même choix ? Ainsi, que rétorquer à un employeur qui a confié à la « sagesse » de l'ordinateur, le soin de décider de l'engagement de telle ou telle personne, après avoir comparé des milliers de CV, procédé à l'analyse des mouvements des visages pendant les interviews, à celle de l'écriture, à la frappe sur les touches de l'ordinateur ?… Rien si ce n'est la déresponsabilisation de l'humain face à la machine.

À ces arguments, on ajoutera la satisfaction de chacun d'entre nous. Nous aimons que notre plateforme musicale nous connaisse et puisse nous guider vers des morceaux qui ont notre préférence ou Amazon vers des produits qui correspondent à nos besoins ; nous aimons, cela nous sécurise, que nos médecins utilisent des systèmes perfectionnés qui garantissent mieux que sa science et son cerveau la détection précoce d'une maladie et que notre mobilophone reconnaisse nos voix, traduisent automatiquement nos messages vocaux ou textuels, nous conduisent à bon port, etc. Les exemples pleuvent.

4. Ainsi, le profilage gagne tous les domaines d'activité de nos entreprises et administrations et nos usages. Les systèmes vous proposent à vous conducteur, la meilleure route à suivre ; à vous chercheur, la façon dont votre indice H pourra évoluer ; à vous responsable d'une commune, les zones d'insécurité ou d'abandon, où votre police doit intervenir ; à vous ministre de l'éducation ou enseignant, les critères selon lesquels *a priori*, les enfants ont des chances de réussir leur parcours scolaire ; à vous juges, les risques de récidive d'une personne auteur d'une infraction ou la décision la plus conforme au droit ou plutôt ce qui a déjà été jugé comme conforme au droit ; à vous lecteur, les ouvrages qui doivent correspondre à vos goûts.

Merci à l'IA et au profilage qu'elle permet et qui nous assure d'avoir un service, plus adapté à notre individualité. Cependant il y a un hic. Les utilisations de l'IA par les acteurs qui nous entourent et en particulier par certains parmi ces acteurs engendrent des risques pour nos libertés individuelles, celles protégées par le droit à la protection des données, moyen au service de toutes nos libertés individuelles : libertés d'expression, d'opinion, de religion, d'association, de déplacement, etc. Au-delà, on découvre que ces systèmes touchent à des enjeux sociétaires : la justice sociale, le développement durable, le pluralisme culturel… et la démocratie. L'Europe en semble consciente et appelle par un recours à l'éthique finalement à une réglementation qui va bien au-delà des seules préoccupations individualistes consacrées par les législations de protection des données. Nous y viendrons plus tard.

On connaît les risques qu'encourent nos libertés individuelles, ceux auxquels précisément le RGPD entend répondre. On sait combien les systèmes d'intelligence artificielle travaillent sur des données, qui ne sont jamais qu'une réduction de la réalité vécue par nous et sont traitées de manière décontextualisée. La mémoire de nos ordinateurs, sans comparaison avec celle limitée de nos mémoires humaines, crée un risque de stigmatisation. L'ubiquité de l'internet des objets et leur portabilité entraînent le risque d'une surveillance continue et de tous les instants et abolissent les frontières de nos espaces privés[2]. Risque nouveau, celui de la manipulation. Comme nous l'avons déjà souligné, les profils créés constituent des outils non seulement d'analyse du passé mais du fait de la « vérité » que ces profils prétendent refléter, une vérité, certes, cette vérité est purement statistique et non exempte de biais, voire d'erreurs. Il est donc intéressant d'utiliser ces profils comme un instrument de prévision de nos comportements futurs (acheter

[2] Il ne s'agit pas simplement de spywares mais de l'ensemble des capteurs, détecteurs en tout genre qui m'accompagnent dans mes lieux intimes, l'enceinte connectée en étant un bel exemple. Pour y remédier, deux pistes : la première instaurer un droit à la déconnexion, la possibilité à tout moment de débrancher le terminal, qu'il s'agisse du mobile, du lecteur de tag, de l'implant corporel, etc. ; la seconde, considérer, comme l'affirmait en 2008, la Cour constitutionnelle allemande, que l'équipement terminal est un domicile virtuel à traiter comme le domicile physique, à savoir un lieu où on ne pénètre qu'avec le consentement de l'occupant.

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

tel produit) ou d'états futurs (une maladie, une intelligence hors du commun)[3]. On ajoute que les *business models* des plateformes, fondés sur l'économie de l'attention, c'est-à-dire la maximisation du profit publicitaire par la rétention de l'internaute le plus longtemps possible sur le service offert conduisent ces plateformes à utiliser des systèmes IA pour envoyer le « bon » message à l'internaute, celui qui accrochera son attention et l'amènera à diffuser à son tour le message. C'est notamment toute la technique des « bulles de filtre » et des « chambres d'écho » qui sont à la base de désinformations massives, qu'elles soient à visée politique ou en matière de santé, comme en ses temps de COVID 19.

5. Ces risques de manipulation, comme le montre le cas *Cambridge Analytica*, sont loin d'être purement individuels. Il touche la collectivité voire nos démocraties. On conclura de même en ce qui concerne les risques de discrimination. La possibilité que le raisonnement automatisé soit entaché de ce qu'il est convenu d'appeler des biais a été longuement évoquée. Ces biais, qu'ils soient volontaires ou non, peuvent conduire à de possibles discriminations. Le poids trop important accordé à un critère, le fait que tel critère utilisé cache un autre critère « discriminant » une catégorie de populations (les noirs, les femmes, les étrangers, les handicapés, les pauvres…) et ce, bien au-delà des critères liés aux catégories de données sensibles ou particulières énoncées par l'article 6 de la Convention 108+, le refus ou au contraire la surpondération d'un élément contextuel spécifique à la personne ou à un groupe concerné, dès lors victime de l'automaticité de l'ordinateur, constitue un dernier risque. Ce risque de discrimination est vécu tant individuellement, que, le cas échéant, par tout un groupe et donc devient un risque collectif : ainsi, l'analyse par un système d'IA des quartiers susceptibles de favoriser une population criminogène met en cause non seulement, à titre de personnes, les personnes physiques de ce quartier, mais également le quartier comme tel, son image et entraîner des conséquences sociales (personnes désertant le quartier ou refusant de s'y installer) voire la surveillance accrue de la police. Les traitements affectent d'autres valeurs que les seules libertés individuelles, en particulier *la justice sociale ou la diversité culturelle* entre individus ou entre groupes et, au-delà, de manière parfois importante, le fonctionnement de nos sociétés et en particulier de notre démocratie. Ainsi, par exemple, la manipulation abusive des individus met en cause tant les libertés que la dignité humaine au sens kantien du terme mais si elle concerne en cela chacun de nous, elle peut également s'étendre à toute une population ou avoir des effets sur l'ensemble de la société. Par ailleurs, l'individualisation de l'offre de services, l'exclusion de certaines personnes du bénéfice de ces services atteignent au-delà des individus des groupes de personnes et soulèvent des questions de justice sociale. Prenons l'exemple des assurances « *one to one* » qu'il s'agit d'assurances soins de santé ou de responsabilité civile, l'individualisation des primes au plus près des « risques » que peut représenter chaque personne, risques calculés en fonction de leur profil, soumet à dure épreuve le sacro-saint principe de la mutualisation des risques pilier de notre système d'assurance. Enfin que dire du *risque de déshumanisation* : l'autonomie de raisonnement et décisionnelle que l'homme confie ou pourrait confier à la machine peut conduire à substituer sa décision automatisée à un raisonnement humain fait de dialogue et d'attention à l'autre. Cette délégation à la machine engendre une préoccupation éthique majeure, tant elle diminue le rôle joué par les personnes et, au-delà, par l'humain.

6. Il est remarquable qu'on déborde ainsi les questions traditionnelles de protection des données ou de vie privée, au sens étroit du terme. La même réflexion peut être adressée à un système d'intelligence artificielle qui aurait pour but de prédire les chances de réussite scolaire ou les risques familiaux d'enfants battus et en arriverait à identifier le poids de certaines données. Cette identification ne pose pas seulement un risque individuel mais bien collectif, dans la mesure où elle risque de stigmatiser certains types de population.

Cette volonté d'élargir la réflexion sur le profilage au-delà des libertés individuelles est présente dans tous les documents sur l'IA et l'éthique produits par les organisations internationales. Je cite l'OCDE qui, dès 2019, a émis

[3] Une première manifestation de cette manipulation réside certainement dans ce qu'il est convenu d'appeler les *nudges*. La théorie du *Nudge* (ou théorie du paternalisme libéral), nous explique Wikipedia, est « *un concept des sciences du comportement, de la théorie politique et d'économie issu des pratiques de design industriel, qui fait valoir que des suggestions indirectes peuvent, sans forcer, influencer les motivations, les incitations et la prise de décision des groupes et des individus, au moins de manière aussi efficace sinon plus efficacement que l'instruction directe, la législation ou l'exécution* ».

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

des recommandations en la matière[4], l'UNESCO qui prépare une convention internationale[5], le Conseil de l'Europe qui vient de sortir le rapport dit de faisabilité du CAHAI[6] et, surtout, la récente Résolution et le projet de règlement émis par le Parlement européen, le 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes[7], qui contient nombre de règles juridiques.

7. Le préambule de la recommandation de l'OCDE est particulièrement clair à ce sujet : « *Les acteurs de l'IA devraient respecter l'état de droit, les droits de l'homme et les valeurs démocratiques tout au long du cycle de vie des systèmes d'IA. Ces droits et valeurs comprennent la liberté, la dignité et l'autonomie, la protection de la vie privée et des données, la non-discrimination et l'égalité, la diversité, l'équité, la justice sociale, ainsi que les droits des travailleurs reconnus à l'échelle internationale* ». On cite dans le même sens d'un élargissement des *préoccupations* au-delà de la protection des données à caractère personnel et des libertés individuelles, le projet de règlement européen du Parlement européen : « *L'intelligence artificielle, la robotique et les technologies connexes, y compris les logiciels, les données et les algorithmes utilisés ou produits par ces technologies, qui comportent un risque élevé d'enfreindre les principes en matière de sécurité, de transparence, de responsabilité, d'absence de biais ou de discrimination, de responsabilité sociale et d'équilibre hommes-femmes, de respect de l'environnement et de durabilité, de vie privée et de gouvernance doivent être considérées comme étant à haut risque relativement au respect des principes éthiques lors de la conclusion d'une évaluation des risques impartiale, réglementée et externe par un organisme national de surveillance* ».

Les capacités en particulier prédictives offertes dès maintenant par l'IA justifient l'interrogation de nos sociétés sur les limites à imposer aux concepteurs et exploitants publics et privés de systèmes d'intelligence artificielle au nom de valeurs éthiques essentielles. Ce point est majeur et soulève la question de la possibilité de lutter contre ces risques collectifs et sociétaux via les textes de protection des données et les organes créés par ces législations. La portée de ces textes et la compétence de ces organes ne sont-ils pas limitées à la seule protection des risques individuels ?

II. La réponse du RGPD – de quelques lacunes[8] !

8. Il ne peut être question dans le cadre de cette courte contribution d'analyser toutes les dispositions du RGPD[9] et de les appliquer à notre sujet mais de souligner les points majeurs de difficulté rencontrés précisément lors de cette application. Le plan du chapitre suit la structure du RGPD. Ainsi, l'adéquation des définitions y compris de la liste des acteurs sera d'abord examinée ; le deuxième point concernera les principes de légitimité des traitements décrits aux articles 5 et 6 ; le troisième, final, s'attardera à quelques obligations significatives du responsable du traitement dont la lecture devra être interprétée à la lumière des particularités des systèmes d'IA. Le projet de recommandation du Conseil de l'Europe adopté par le Conseil consultatif de la Convention n° 108 et soumis au Conseil des ministres[10], à

[4] Recommandation du Conseil sur l'intelligence artificielle, adoptée par le Conseil des ministres de l'OCDE, le 22 mai 2019, disponible à l'adresse suivante : https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449.

[5] Rapport préliminaire sur l'Avant-projet de recommandation sur l'éthique de l'intelligence artificielle, disponible à l'adresse : https://unesdoc.unesco.org/ark:/48223/pf0000374266_fre.

[6] CAHAI (Comité *Ad Hoc* Artificial Intelligence dont les travaux sont accessibles sur la page : www.coe.int/cahai), *Étude de faisabilité relative à un cadre juridique pour la création, le développement et l'application de l'IA sur la base des normes du Conseil de l'Europe*, 17 décembre 2020, disponible à l'adresse : https://rm.coe.int/cahai-2020-23-final-etude-de-faisabilite-fr-2787-2531-2514-v-1/1680a1160f.

[7] Résolution du Parlement européen du 20 octobre 2020 déjà citée, contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes (2020/2012(INL)).

[8] Cette partie reprend des réflexions émises dans le rapport B. Frenay – Y. Poullet, *Profiling and Convention 108+: Report on developments after the adoption of Recommendation (2010)13 on profiling*, rapport établi pour le Conseil consultatif de la Convention n° 108, novembre 2019 dans le cadre de la révision de la recommandation de 2010 sur le profilage, rapport à paraître.

[9] V. EDPB, Lignes directrices sur la prise de décisions individuelles automatisées et le profilage aux fins du règlement 2016/679 (wp251rev.01), 22 août 2018, accessible sur le site de l'EDPB déjà cité. On citera également l'étude comparative réalisée dans le cadre du Fundamental Rights and Citizenship Programme of the European Commission : Protecting citizens' rights against illicit profiling-*Comparative report on automated profiling in 28 EU member states and Switzerland*, accessible à l'adresse : www.statewatch.org/media/documents/news/2014/nov/profiling-project-ws.pdf.

[10] Draft Recommendation on the protection of individuals with regard to the processing of personal data in the context of profiling (revising Recommendation (2010)13), 24 février 2021, T-PD(2019)07BISrev6, Comité consultatif de la Convention n° 108 relatif à la protection des individus au regard des traitements automatiques de données

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

la rédaction duquel nous avons eu le plaisir de contribuer, servira de guide dans nos réflexions.

A. *Les définitions*

9. La première réflexion interroge le champ d'application du RGPD. Le texte circonscrit aux seules données à caractère personnel ses dispositions. Il nous paraît que cette restriction pose problème, du moins dans le cadre de nombre de systèmes d'intelligence artificielle L'argument est double. Premièrement, il note que la puissance de certains systèmes d'IA est telle que des données, pourtant considérées comme rendues anonymes, peuvent être re-personnalisées[11]. Deuxièmement, on souligne que la plupart des systèmes d'IA, en particulier de profilage, utilisent des données anonymes, ainsi dans le cadre d'un profilage permettant de sélectionner les candidats à un logement, l'opérateur d'un système se référera à des données telles que le revenu moyen des personnes originaires de tel quartier, le niveau scolaire des habitants ou leur niveau d'endettement. Limiter les dispositions du RGPD aux seules données à caractère personnel représente dès lors un risque en matière de transparence pour la personne concernée : il est requis d'envisager également les *données anonymes* qui, dans bien des cas, peuvent également servir à la constitution du profil. Ainsi, conformément aux articles 13, 14 et 15 du RGPD, limiter l'information et l'accès à la personne concernée aux seules données à caractère personnel intervenues dans la fabrication de son profil de candidat à l'emploi et exclure de cette information les données anonymes apparaîtrait comme une information incomplète voire biaisée[12]. Le RGPD repose également sur la distinction qu'il introduit, au sein des données à caractère personnel, par la création de catégories spéciales de données énumérées à l'article 9 et qui font l'objet de dispositions protectrices renforcées. Nous insistons sur le fait que les prédictions de l'IA permettent de déduire de données, par nature anodines, des informations sensibles. Cambridge Analytica et les exemples donnés (*supra*, n° 2) à propos de prédictions relatives à la santé témoignent de l'intérêt d'une définition à la fois par la nature et par la finalité de ces catégories particulières de données.

10. Le montage d'un système d'intelligence artificielle ou l'exploitation de celui-ci requiert dans la plupart des cas l'intervention de multiples acteurs : ainsi, à côté de celui qui souhaite utiliser le système, on ajoute souvent les fournisseurs d'algorithmes, ceux de données, les intégrateurs qui adapteront le système aux besoins de l'utilisateur. Par ailleurs, les plateformes, par la richesse des données qu'elles collectent, jouent un rôle important soit dans la fourniture des données répondant aux spécificités des besoins de profilage de ses clients, soit, sur la base de ce cahier des charges, appliqueront les algorithmes *ad hoc* et sur la base de la sélection opérée, communiqueront les « cibles » susceptibles d'être intéressées par le produit ou le service du client. L'intervention de ces différents acteurs pose la question de la qualification de chacun au regard des législations de protection des données. Les définitions du RGPD distinguent principalement deux concepts. Le responsable de traitement qui, selon l'article 4.1., définit les finalités et les moyens du traitement. Le responsable peut être unique ou être conjoint. Le sous-traitant, apparaît en aval du responsable du traitement. Il traite les données dans le cadre de tâches confiées par le responsable. Cette typologie apparaît bien insuffisante au regard des multiples rôles nécessaires au montage ou à l'exploitation des systèmes d'IA. Ainsi, comment qualifier le fournisseur d'un algorithme ou de données, qui interviennent en amont de la création du système ? Les textes relatifs à l'éthique de l'IA dont nous avons parlé plus haut (*supra*, n° 7) tiennent compte de la nécessité d'élargir la responsabilité des acteurs qui peuvent difficilement être qualifiés de responsable ou

personnelles. Révision de la recommandation (2010)13). Dans la suite du texte, nous nous référerons à ce texte sous les termes de projet de recommandation du Conseil de l'Europe.

[11] À cet égard, à propos des données de communications téléphoniques rendues anonymes, « On the privacy-conscientious use of mobile phone data », *Scientific Data, No 5*, 11 December 2018 (https://www.nature.com/articles/sdata2018286.pdf).

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

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

sous-traitant. Ainsi, les recommandations de l'OCDE[13] et, plus récemment, la Résolution du Parlement européen[14] plaident pour un élargissement des obligations de chaque acteur qui, de près ou de loin, participe de manière essentielle à la conception, à la mise sur pied et à l'exploitation des outils d'IA. Ainsi, les fournisseurs des algorithmes ou de données doivent s'assurer de la qualité de leurs fournitures et collaborer en cas de problème avec les responsables ou sous-traitants. Autre point celui des plateformes, à la suite d'un arrêt de la Cour de justice de l'Union européenne (CJUE)[15], les récentes lignes directrices sur le « ciblage » des utilisateurs des réseaux sociaux énoncées par l'EDPB[16] confirment la jurisprudence de la Cour et examinent en particulier les différentes méthodes utilisées par les entreprises et les plateformes de réseaux sociaux pour cibler leur clientèle, 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 et permet l'accès électif à sa base de données. L'EDPB en déduit la nécessité selon l'article 26.2 d'une convention entre eux à propos de la répartition des obligations mises à charge des responsables de traitement : « *In terms of scope, the EDPB considers that the arrangement between targeters and social media providers should encompass all processing operations for which they are jointly responsible (i.e. which are under their joint control). By concluding an arrangement that is only superficial and incomplete, targeters and social media providers would be breach of non-compliance with their obligations under Article 26 of the GDPR* ».

B. *Les principes*

11. Les principes énumérés à l'article 5 du RGPD et les causes de licéité des traitements énumérées par l'article 6 sont bien connus. Le principe de loyauté s'entend notamment d'une information des personnes concernées sur toute une série de caractéristiques du traitement. Cette information s'avère difficile vis-à-vis de tiers dont les données sont incidemment collectées[17]. Les types de données collectées peuvent être nombreux (v. par exemple, en cas de voiture intelligente). Surtout, on souligne la grande hétérogénéité des sources. Il importera de les lister dans le cadre de l'information due à la personne concernée. Surtout, le fait que le système, par les qualités caractéristiques des systèmes d'IA, puisse prédire et décider vis-à-vis d'une personne entraîne des devoirs d'information complémentaires. On sait que l'article 13.2, f), du RGPD a ajouté à la liste des informations dues en cas de « *décision automatisée y compris un profilage* », l'existence de celui-ci[18] mais également, l'« *impact potentiel du profilage sur la personne concernée* » et enfin, des « *informations utiles (meaningful) sur la logique sous-jacente* ». Concernant cette « *logique sous-jacente* »[19], nous reviendrons

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

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

[15] CJUE, 29 juillet 2019, *Fashion ID c. Verbraucherzentrale*, aff. C-40/17, points 79 et s.

[16] EDPB, *Guidelines 8/2020 on the targeting of social media users*, Version 1.0, Adopted on 2 September 2020, en particulier p. 17.

[17] Ainsi, dans le cadre d'un robot aide-soignant, les images prises de visiteurs du patient à domicile ou hospitalisé.

[18] Notre rapport au Conseil de l'Europe suggère que celui-ci puisse se faire par une icône placée sur le site. Cliquer sur l'icône renverrait alors à une page où l'ensemble des informations nécessaires seraient présentes.

[19] Sur le commentaire des termes « *logique sous-jacente* », utilisés par le RGPD, on lira les *Guidelines on Automated individual decision-making and Profiling*, publiées par le Groupe de travail de l'article 29 et depuis reprises par l'EDPB, le 3 octobre 2017 et revues le 6 février 2018, WP251rev.01 (texte disponible en anglais sur le site de l'EDPB : https://edpb.europa.eu/edpb_en) : « *Data controllers should find simple ways to tell the data subject[s] about the rationale behind, or the criteria relied on in reaching the decision[s] […] but] not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm. The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision* ».

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

sur le choix des termes[20]. À ce stade, relevons que les systèmes d'IA utilisant des systèmes de *machine learning* ne suivent pas une « logique » mais simplement des modèles statistiques. L'OCDE[21] décrit comme suit l'objectif des mesures d'information en cas d'utilisation d'un système de profilage utilisant l'IA (Recommandation 1.3 : « transparence et explicabilité ») : « *Les acteurs de l'IA devraient s'engager à assurer la transparence et une divulgation responsable des informations liées aux systèmes d'IA. À cet effet, ils devraient fournir des informations pertinentes, adaptées au contexte et à l'état de l'art, afin :*

i. de favoriser une compréhension générale des systèmes d'IA,

ii. d'informer les parties prenantes de leurs interactions avec les systèmes d'IA, y compris dans la sphère professionnelle,

iii. de permettre aux personnes concernées par un système d'IA d'en appréhender le résultat, et,

iv. de permettre aux personnes subissant les effets néfastes d'un système d'IA de contester les résultats sur la base d'informations claires et facilement compréhensibles sur les facteurs, et sur la logique ayant servi à la formulation de prévisions, recommandations ou décisions ».

Enfin, toujours en vertu du principe de loyauté, des textes récents[22] ont affirmé l'obligation des organisations, qui utilisent des robots humanoïdes, de révéler leur qualité non humaine et la nécessité de pouvoir toujours distinguer leur nature au premier coup d'œil, par exemple par la présence d'une icône de signalement.

12. La détermination des finalités exigée par le RGPD rencontre dans le cas des systèmes IA des difficultés d'application. Ainsi, le responsable du traitement, au hasard des agrégations de données permises par le *big data* et ses algorithmes peut assigner facilement des objectifs nouveaux. Prenons quelques exemples : le profilage de la clientèle peut, dans un premier temps, avoir pour seule finalité la sélection de la clientèle, l'affinement du système peut amener à avoir une meilleure connaissance des potentiels clients ainsi sélectionnables et sur cette base de leur proposer des prix différenciés en fonction d'indices de leur demande potentielle pour tel ou tel produit. Autre exemple, si Facebook développe pour son propre intérêt un système d'analyse intelligente des données de l'utilisation de son réseau social, elle offre également à des « partenaires », par son système d'IA, des accès ciblés à ses blogs et leur permet ainsi de mieux connaître leurs potentiels « clients » ou utilisateurs[23]. Il nous apparaîtrait dangereux qu'à ces occasions le responsable du traitement invoque l'existence de finalités compatibles, définies strictement par l'article 6.4 du RGPD.

Enfin, les risques liés à l'impact dans certains secteurs de certains traitements de profilage utilisant l'IA peuvent amener à interdire *a priori* leur utilisation à certaines finalités. On cite les craintes d'utilisation de la reconnaissance faciale et dès lors la réglementation stricte qui s'y applique[24]. Récemment, la loi belge sur les

[20] Et ce, à propos de l'article 22 du RGPD (*infra*, n° 22) qui concerne les droits de la personne concernée en cas de décisions automatisées.
[21] OCDE, Recommendation on Artificial Intelligence (AI) – the first intergovernmental standard on AI –, adopté par le Conseil des ministres de l'OCDE, le 22 mai 2019.
[22] Ainsi, le rapport du HLGE on Artificial Intelligence déjà cité p. 34 : « *Human beings should always know if they are directly interacting with another human being or a machine, and it is the responsibility of AI practitioners that this is reliably achieved. AI practitioners should therefore ensure that humans are made aware of – or able to request and validate the fact that – they interact with an AI system (for instance, by issuing clear and transparent disclaimers). Note that borderline cases exist and complicate the matter (e.g. an AI-filtered voice spoken by a human). It should be borne in mind that the confusion between humans and machines could have multiple consequences such as attachment, influence, or reduction of the value of being human.73 The development of human-like robots74 should therefore undergo careful ethical assessment.*" Ce principe de 'distinction' interdit toute utilisation non transparente des technologies pour faire croire artificiellement à l'action d'une personne, telle que stigmatisée par la Déclaration de Montréal (Principe d'intimité et de vie privée, n° 8) : « *L'intégrité de l'identité personnelle doit être garantie. Les SIA (Systèmes d'intelligence artificielle) ne doivent pas être utilisés pour imiter ni modifier l'apparence physique, la voix et d'autres caractéristiques individuelles dans le but de nuire à la réputation d'une personne ou pour manipuler d'autres personnes* » (Déclaration de Montréal. Pour une IA responsable, Déclaration développée sous les auspices de l'Université de Montréal, 2017, www.declarationmontreal-iaresponsable.com/la-declaration).
[23] Le rapport de l'ICO (ICO, *Big Data, artificial intelligence, machine learning and data protection*, p. 11, disponible à l'adresse suivante : https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf) *Big Data, artificial intelligence, machine learning and data protection* (dernière consultation, 17 janvier 2021), l'autorité de protection des données, donne l'exemple de la société Data Sift. Cette société à partir de données venant de Twitter, Facebook et autres médias sociaux qu'elle analyse et revend pour des finalités marketing ou autres.
[24] Ainsi, en France, la reconnaissance faciale pour le compte de l'État peut être justifiée par l'intérêt public (*article 6 III de l'Ordonnance de 2018*). Elle doit être autorisée par décret en Conseil d'État après avis de la CNIL, lorsqu'elle : 1. Intéresse la sûreté de l'État, la défense ou la sécurité publique ; 2. A pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté. (*Article 31 II de*

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

assurances a été modifiée le 4 décembre 2020. L'article 4.2 prévoit : « *Lors de la conclusion du contrat visé à l'article 46/1, le refus du candidat assuré d'acquérir ou d'utiliser un objet connecté qui récolte des données à caractère personnel concernant son mode de vie ou sa santé ne peut en aucun cas conduire à un refus d'assurance ni à une augmentation du coût du produit d'assurance* ». Et l'article 5 introduit un article 46.3 qui énonce : « *Aucune segmentation ne peut être opérée sur le plan de l'acceptation, de la tarification et/ou de l'étendue de la garantie sur la base de la condition que le candidat assuré accepte d'acquérir ou d'utiliser un objet connecté qui récolte des données à caractère personnel concernant son mode de vie ou sa santé, accepte de partager des informations récoltées par un tel objet connecté, ni sur la base de l'utilisation par l'assureur de telles informations* ». On doit s'attendre à une multiplication de telles réglementations spécifiques au vu des risques importants de discrimination que représentent les capacités prédictives et décisionnelles de l'IA.

13. Les principes de minimisation et de proportionnalité de la durée présupposent que l'on puisse *a priori* déduire de la finalité de l'application les données nécessaires à son obtention et la durée de leur conservation. Or les systèmes dits de *machine learning* fonctionnent grâce à des corrélations statistiques établies sur la base de rapprochements souvent non prévisibles de données et exigent donc que les réservoirs de données brassent très largement[25]. Le projet de recommandation du Conseil de l'Europe sur le profilage recommande au moins la balise des « *legitimate expectations* »[26] Sans doute cette balise est-elle insuffisante et faudra-t-il, secteur par secteur avec le cas échéant des interventions législatives fixant elles-mêmes certaines limites aux données utilisées, répondre à des questions, qui sont loin d'être triviales comme les suivantes : « *Jusqu'où, une compagnie d'assurances peut-elle utiliser des données relatives aux personnes assurées dans le cadre de l'offre de services individualisés ?* » ; « *Jusqu'où une banque ou un organisme de crédit peut-il au nom de sa responsabilité de donneur de crédit et suivant les exigences du principe 'Know your customer' profiler ses clients ?* » ; « *Dans quelle mesure, un employeur peut-il utiliser, vis-à-vis des employés ou candidats employés, des systèmes d'affective computing dans le cadre de leur sélection, gestion de carrière, etc. ?* ».

14. Un mot sur le consentement comme cause de licéité des traitements. La formule souvent trompeuse à moins qu'elle ne soit ironique, des opérateurs des sites web : « *Nous sommes soucieux de votre vie privée* »… qui se termine par l'invitation à un « *J'accepte* », les cookies que vous me proposez, faute de quoi je ne pourrai accéder à la richesse de votre site, illustre bien les dangers du consentement comme base de licéité des traitements. Le consentement via l'acceptation de cookies sera obtenu de manière globale ou à travers un paramétrage de vos préférences, fastidieux et souvent aux critères incompréhensibles. Répond-il aux exigences du RGPD ? Ces dernières réclament un consentement libre, éclairé et spécifique[27]. Tout cela dit, soulignons que les qualités requises du consentement seront rarement remplies. Elles supposent, sous réserve d'autres exigences encore, un consentement libre, c'est-à-dire non manipulé et sur la base d'un choix réel qui puisse être autre que le seul : « *j'accepte* ». La complexité des montages des systèmes supportés par les technologies de l'IA, la diversité des sources utilisées, l'impossibilité de prévoir les corrélations qui seront à la base des décisions du responsable et, dans le contexte de l'accès à des services gratuits et à portée d'un clic, la difficulté de prendre le recul nécessaire au moment où on pousse sur le « j'accepte », tous ces facteurs rendent les conditions mises par le RGPD complètement illusoires d'autant

l'Ordonnance) ; 3. Est nécessaire à l'authentification ou au contrôle de l'identité des personnes, et que l'État agit dans l'exercice de ses prérogatives de puissance publique. (*Article 32 de l'Ordonnance*).

[25] Ainsi, hypothèse purement fictive, il pourrait apparaître, aux yeux de l'administration fiscale lors de l'utilisation de vastes banques de données, que les dirigeants d'entreprise de plus de 200 employés et moins de 400, disposant d'une voiture rouge immatriculée entre telle et telle année, ayant l'habitude de voyages « *all inclusive* » dans les pays méditerranéens, habitant tel type de quartier dans des villes de plus de 50 000 habitants, avec un enfant et un chien, constituent des fraudeurs potentiels.

[26] « *Les données personnelles utilisées dans le cadre du profilage devraient être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles seront traitées. Dans les systèmes de "machine learning" il est difficile de connaître* a priori *quelles données permettront des corrélations significatives. Par ailleurs, il est important de limiter le traitement de profilage à des catégories de données dont la personne concernée peut raisonnablement s'attendre (légitimement s'attendre) à ce qu'elles soient prises en considération au vu des finalités du profilage* ».

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

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

plus que le refus peut conduire à un non accès au service. 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, comme l'accès aux très larges[28] plateformes de réseaux sociaux ou d'informations.

15. Quelles solutions proposer ? On peut imaginer que le profilage soit lié aux nécessités de service lui-même, ainsi si vous souhaitez que Spotify vous offre un choix musical qui correspond à vos préférences. Dans ce cas, ce sont les nécessités de l'exécution du contrat qui constituent la base de licéité du traitement et non le consentement. On ajoute que dans ce cas, la personne concernée devrait avoir le choix entre, d'une part, le service de base non profilé, qui n'exige aucun traitement de vos données et s'appliquerait par défaut, et, d'autre part, le service profilé[29]. Peut-on imaginer que les responsables fassent payer le coût que représente pour eux le non-profilage. On sait que le modèle économique de la gratuité des services offerts engendre les dérives, en particulier celles justifiées par l'économie de l'attention. Il m'apparaitrait donc acceptable de prévoir cette rémunération, sur base d'un calcul « *cost-based* », c'est-à-dire le calcul de la perte des bénéfices raisonnables attendus de la publicité profilée. Reste à savoir si nos autorités publiques disposent des informations pour ce calcul et des moyens pour faire respecter le prescrit. Sans doute, est-ce du côté du droit de la consommation qu'une réflexion doit être menée en la matière. Cette incursion dans (ou plutôt cette synergie avec) le droit de la consommation pourrait être bien utile à propos d'une deuxième solution, à savoir la négociation collective entre les responsables de traitement et les représentants de leurs clients sans doute avec la médiation des autorités de protection des données.

C. *Les droits de la personne concernée*

16. L'analyse du principe de loyauté conduisait déjà à reconnaître le besoin d'un élargissement des informations à communiquer et par là du droit d'accès. En particulier, la cession ou le partage des données ou des profils à des tiers doivent faire l'objet d'une information spécifique et il serait utile d'ouvrir un droit d'opposition non motivée au-delà de celui reconnu par l'article 21.2, limité aux traitements à des fins de prospection. Les risques liés à de tels cessions ou partages justifient une telle innovation. Dans un ouvrage récent, Y. Meneceur[30] soulignait l'exemple d'une société de grande distribution anglais disposant d'une mégadonnées, ayant cédé à la police un grand nombre de données. Cette cession était d'autant plus contestable qu'elle avait lieu dans le cadre du projet HART (*Harm Assessment Risk Tool*) qui visait à prévenir la commission d'infractions.

17. C'est surtout à propos de l'article 22 du RGPD déjà évoqué (*infra*, n° 11) que des demandes de précision sont absolument nécessaires au regard des réalités du fonctionnement des systèmes de *deep learning*. L'article 22 du RGPD consacre le droit de la personne concernée « *de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* ». L'analyse de cette disposition laisse apparaître nombre de lacunes ou, en tout cas, d'ambiguïtés. Que veulent dire les expressions : « *décision fondée exclusivement* »[31] ; « *affecter de manière significative* » et le terme « *uniquement* » ? Enfin, la décision dont parle l'article 22 doit viser une « *personne concernée* ». C'est la conséquence certes d'une législation centrée sur la protection de personnes individuelles mais ne

[28] C'est ainsi que le projet européen de Digital Services Act qualifie les plateformes détenant un marché couvrant au moins 10 % de la population européenne, comme Twitter, Instagram, Facebook, YouTube, Google, etc.

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

[30] Y. Menecoeur, *L'intelligence artificielle en procès*, Bruxelles, Bruylant, 2020, pp. 100 et 101.

[31] Ainsi, il suffira que le responsable de traitement argue du fait que la vérité sortie de l'ordinateur est soumise à une révision humaine. On sait que cette possibilité de révision humaine sera souvent purement illusoire, dans la mesure où l'agent du responsable osera difficilement mettre en cause la décision, sous peine d'être jugé responsable au cas où sa décision qui met en cause l'« objectivité » et l'intelligence du système informatique, s'avère malheureuse.

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

faudrait-il pas également prendre en compte le fait que des systèmes en particulier prédictifs visent des catégories de personnes : ainsi les personnes habitant tel quartier, ayant tel type de comportement sur le net, telle mobilité… ? Le risque est ici collectif et, de ce fait, mériterait *a fortiori* d'être pris en compte. Nous ne pourrons dans le cadre de cette contribution analyser tous ces ambiguïtés, voire lacunes[32]. Par ailleurs, l'article 22.2 prévoit des exceptions qui s'appliqueront facilement à la plupart des systèmes d'IA : besoins contractuels ou précontractuels, consentement de la personne concernée ou exécution d'une mission d'intérêt public autorisée par l'État.

Précisément à propos de ces exceptions, on déplore que le texte reste flou et peu adéquat quand on connaît les conséquences de certains profilages. La disposition évoque simplement le droit à des « mesures appropriées » et à l'obtention d'une intervention humaine. Certes, l'intervention humaine ne peut se limiter à une simple réaffirmation par oral de la 'vérité sortie de l'ordinateur' mais à partir de quand pourra-t-on considérer que l'humain a une réelle capacité de remise en cause de la présomption de vérité sortie des ordinateurs[33] ? Que recouvrent les termes « *garanties appropriées* » : le droit à une audience en face à face ? Un droit de contestation de la décision après explication ? Ne peut-on suivre les exigences du considérant n° 71 qui exige que le bénéfice de ces exceptions de l'article 22.2 soit assorti par ceux qui s'en prévalent « *de garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision* ». Ainsi, le responsable se devra, suite à une décision prise, d'offrir, non seulement, une interface humaine capable de recevoir la personne concernée et de répondre à ses questions mais également de donner toutes les informations qu'il détient dans le cadre des exigences d'« explicabilité » de la décision prise[34], c'est-à-dire au minimum les bases suffisantes pour permettre la compréhension du processus, qui a mené à la décision prise, et la possibilité, dès lors, pour la personne concernée, de la contester en connaissance de cause. Cette possibilité de contester doit s'entendre de la possibilité d'un recours à l'autorité de protection des données certes mais, également, d'un recours interne auprès d'une personne ayant compétence de revoir les décisions prises par ou à la suite de l'utilisation du système de *machine learning*[35].

18. Un autre droit nous semble devoir être consacré au profit des personnes concernées : le droit à des terminaux fiables et au fonctionnement transparent dans leur collecte des données. L'internet de plus en plus ubiquitaire des objets au fonctionnement opaque (par exemple, qu'enregistrent nos enceintes connectées ? et à qui les transmettent-elles ?) est un fait qui conduit à devoir reconnaître ce droit.

D. *L'obligation du responsable de procéder à un « Privacy Impact Assessment » voire à un « Ethical Values Assessment »*

19. Pour les traitements présentant un *risque élevé* pour les personnes concernées, l'article 35 du RGPD prescrit aux responsables de traitement l'obligation de procéder à une évaluation des risques (en abrégé *PIA*). L'article liste les critères qui conduisent à qualifier le traitement comme présentant ce risque élevé Il s'agit, selon le RGPD, de procéder à une évaluation interne des risques en matière de protection des données et la présentation des mesures prises pour atténuer le risque. Sans nous livrer à une analyse détaillée de cet article et de

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

[33] Sur cette « incontestabilité » de la décision produite par la machine, lire, entre autres, M. Kaminsky, « *And where human decision-making can often be contested, algorithmic decision-making (…) is often taken at face value, and left unchallenged and unchallengeable* ». (« Binary governance: lessons from the GDPR's approach to algorithmic accountability », *Southern California Law Review*, 2019, 76, p. 15.

[34] Comme l'affirme le Groupe de l'article 29 dans ses Lignes directrices reprises et confirmées par l'European Data Protection Board (Groupe de l'article 29, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679, WP251 rev.01, adoptées le 3 octobre 2017 et révisées le 6 février 2018, p. 18), « *compte tenu du principe fondamental de transparence qui sous-tend le RGPD, les responsables du traitement doivent veiller à expliquer clairement et simplement aux personnes concernées la manière dont fonctionne le profilage ou le processus décisionnel automatisé* », ce qui ne signifie pas « *une explication complexe des algorithmes utilisés* ».

[35] Le projet de recommandation du Conseil de l'Europe prévoit la nomination par le responsable de traitement d'une personne en charge de traiter ces recours internes.

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

son application aux traitements de profilage[36], relevons que ce concept de traitement à « risque élevé » ou à « haut risque » est repris par la proposition de règlement émanée du Parlement européen en matière d'éthique de l'IA, de la robotique et des technologies connexes mais avec une autre acception et surtout une réglementation plus stricte. Ainsi, les risques à envisager concernent tant les risques encourus par nos libertés individuelles que ceux collectifs[37] (v. *supra*, n° 7) comme ceux d'atteinte à l'environnement, à la justice sociale ou à la démocratie[38]. Cette extension aux risques collectifs de la notion de risque élevé nous apparaît utile et, à notre avis, couvre nombre de traitements de profilage[39]. Il s'agit bien soit de passer d'un « *Privacy Impact Assessement* » (PIA) à un « *Ethical values Assessement* », qui comprend ce PIA, soit de maintenir les deux de manière parallèle. Reste, dans les deux hypothèses, à s'interroger sur la manière dont les deux dispositifs et les deux autorités en charge de ces deux évaluations pourront collaborer.

20. Afin de faciliter ou d'anticiper cette évaluation, tant le RGPD que le projet du Parlement européen incitent à la mise sur pied et au recours à des mécanismes de certification et de labellisation des traitements. La référence au texte parlementaire européen suggère l'adoption de mesures plus sévères. Alors que le RGPD se contente d'un contrôle interne, avec le cas échéant, une obligation de consultation de l'autorité de protection des données, le contrôle imaginé par le projet du Parlement européen est confié préventivement à un organisme national de surveillance chargé de l'évaluation des risques éthiques liés à l'IA, externe, indépendant, multidisciplinaire et *multistakholder*s ou à un organisme accrédité par cet organisme[40]. On note, en outre, que ce contrôle préventif suppose l'auditabilité des systèmes d'IA[41] et que l'audit est prévu à des

[36] À cet égard, l'article 1.1, k), de la Recommandation, qui définit les applications de profilage à haut risque comme suit : « *L'expression "traitements de profilage à risque élevé" peut notamment désigner :*
i. le profilage dont le fonctionnement entraîne des effets juridiques ou qui ont un impact significatif pour la personne concernée ou pour le groupe de personnes identifié par le traitement de profilage ;
ii. le profilage qui, en raison du public visé ou du contexte ou de la finalité du traitement, en particulier en raison de la possibilité d'abus ou de détournement du déséquilibre dans le pouvoir d'information, notamment lorsqu'il s'agit de mineurs ou de personnes vulnérables, comporte un risque d'affecter ou d'influencer des personnes concernées ;
iii. le profilage ayant pour objet des données relevant des catégories particulières de données au sens de l'article 6 de la Convention 108+ ou ayant pour finalité de les détecter ou les prédire ;
iv. le profilage affectant un très grand nombre de personnes, notamment celui opéré par des services d'intermédiaires en ligne à leur bénéfice ou pour celui de tiers ».

[37] Pour distinguer les systèmes à haut risque des autres, le Livre blanc de la Commission sur l'intelligence artificielle (« Livre blanc – Intelligence artificielle – Une approche européenne basée sur l'excellence et la confiance », Bruxelles, le 19 février 2020, COM(2020)65 final, disponible sur le site : https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf (consulté pour la dernière fois, le 16 janvier 2021) prend dans le domaine médical (p. 20), l'exemple suivant : l'utilisation d'un système IA pour la fixation des agendas du corps médical d'un hôpital ne présente pas les mêmes risques que l'utilisation d'un système pour la détection préventive des personnes qui pourraient demain souffrir de la maladie d'Alzheimer. « *Si une telle approche est importante pour garantir la proportionnalité de l'intervention réglementaire, elle requiert néanmoins des critères précis pour différencier les diverses applications de l'IA, et notamment pour déterminer si elles sont ou non "à haut risque". Les éléments permettant d'établir qu'une application d'IA est à haut risque devraient être clairs, faciles à comprendre et applicables à toutes les parties concernées* ».

[38] Lire en ce sens, l'article 4, e), du texte du Parlement : « "*haut", un risque important associé au développement, au déploiement et à l'utilisation de l'intelligence artificielle, de la robotique et des technologies connexes de causer du tort ou un préjudice aux individus ou à la société en violation des droits fondamentaux et des règles de sécurité établis par le droit de l'Union, en tenant compte de leur utilisation ou finalité spécifique, du secteur dans lequel elles sont développées, déployées ou utilisées et de la gravité des torts ou des préjudices susceptibles de se produire ;* ». On ajoute que le projet du Parlement liste les traitements en fonction à la fois des secteurs et de la finalité des applications les traitements IA à haut risque.

[39] À cet égard, l'article 1.1, k), de la Recommandation en projet du Conseil de l'Europe définit les applications de profilage à haut risque comme suit : « *L'expression "traitements de profilage à risque élevé" peut notamment désigner :*
i. le profilage dont le fonctionnement entraîne des effets juridiques ou qui ont un impact significatif pour la personne concernée ou pour le groupe de personnes identifié par le traitement de profilage ;
ii. le profilage qui, en raison du public visé ou du contexte ou de la finalité du traitement, en particulier en raison de la possibilité d'abus ou de détournement du déséquilibre dans le pouvoir d'information, notamment lorsqu'il s'agit de mineurs ou de personnes vulnérables, comporte un risque d'affecter ou d'influencer des personnes concernées ;
iii. le profilage ayant pour objet des données relevant des catégories particulières de données au sens de l'article 6 de la Convention 108+ ou ayant pour finalité de les détecter ou les prédire ;
iv. le profilage affectant un très grand nombre de personnes, notamment celui opéré par des services d'intermédiaires en ligne à leur bénéfice ou pour celui de tiers ».

[40] À cet égard, l'article 18 du projet de règlement proposé par le Parlement européen : « *Chaque État membre désigne un organisme public indépendant chargé de contrôler l'application du présent règlement (ci-après "organisme de surveillance") et de réaliser les évaluations des risques et de la conformité et la certification prévues aux articles 14, 15 et 16 sans préjudice de la législation sectorielle* » et l'article 16 : « *Lorsque l'évaluation de la conformité de l'intelligence artificielle, de la robotique et des technologies connexes à haut risque, y compris les logiciels, les données et les algorithmes utilisés ou produits par ces technologies, effectuée conformément à l'article 15, se révèle positive, l'organisme national de surveillance compétent délivre un certificat européen de conformité éthique* ».

[41] Dans le même sens, le projet de recommandation du Conseil de l'Europe sur le profilage déjà cité : « *Aux fins d'une évaluation continue des risques tant individuels que collectifs, et en tout cas lorsqu'il s'agit de traitements de profilage à risque élevé, les responsables du traitement et, le cas échéant, les sous-traitants devraient documenter l'entraînement du modèle et effectuer des évaluations d'impact régulières en traitant des risques spécifiques du profilage basé sur des*

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

intervalles réguliers. On sait que le HLGE a émis sur ce point des lignes directrices[42] autour de 7 principes clés à suivre par les acteurs qui participent à l'élaboration ou à l'exploitation d'un système d'IA[43] et que son secrétariat a traduit les principes ainsi énoncés en une « *Assessment List on Trustworthy Artificial intelligence* »[44]. Il est intéressant de noter que le projet de règlement sur les services numériques (le *Digital Service Act* (DSA))[45] contient des dispositions qui vont dans le sens indiqué par le Parlement. Les articles 26 et 27 de ce projet de règlement requièrent des très larges plateformes qui utilisent des logiciels de profilage tant pour la modération des contenus que pour leurs recommandations des mesures d'évaluation des risques tant individuels que collectifs liés au fonctionnement de ces logiciels[46] et, le cas échéant, l'atténuation de tels risques. Ces mesures doivent être réfléchies avec la participation de représentants des bénéficiaires du service, de représentants de groupes potentiellement touchés par leurs services, d'experts indépendants et d'organisations de la société civile. Les propositions ainsi élaborées doivent ensuite faire l'objet d'un audit externe par un organisme indépendant dont les recommandations devront être prises en compte et, selon l'article 33, publiées semestriellement par la plateforme elle-même avec leur propre évaluation des risques et les mesures d'atténuation prises.

Conclusion

21. Notre contribution avait pour ambition de répondre à la question : le RGPD, cinq ans après, répond-il de manière adéquate aux défis nouveaux que pose l'intelligence artificielle, en particulier dans ses applications en matière de profilage ? La réponse certes ne nie pas l'intérêt des multiples dispositions du RGPD et on salue l'interprétation courageuse apportée par les juges et l'EDPB aux dispositions du texte de manière à répondre à certaines lacunes (la notion de responsables conjoints, l'interprétation large de la notion de données sensibles…) mais certaines lacunes apparaissent cependant[47]. Les définitions tant des données, objet des dispositions du RGPD que des acteurs sont, à notre opinion, trop courtes pour rencontrer les préoccupations de protection des libertés individuelles. Les principes de finalité et de proportionnalité sont mis à rude épreuve et méritent tant une responsabilisation des acteurs de l'IA qu'une attention législative particulière. Sans doute, au-delà, faut-il relever le besoin de passer à propos du profilage, d'une *obligation d'information à celle d'explication et de maîtrise* des systèmes d'intelligence artificielle mais également en ce qui concerne le fonctionnement de nos robots et de tous les objets intelligents qui nous entourent. Comme le note J. Eynard[48], « *On passe ainsi petit à petit d'une obligation d'information à une obligation d'explication ce qui va dans le sens d'une meilleure maîtrise par l'usager des processus mis en œuvre* », tant dans la collecte des informations que leur traitement et les « décisions » qui en sortent. La deuxième est le besoin de renforcement d'une *approche préventive* des risques. Cette approche semble systématiquement s'imposer pour les systèmes

systèmes d'IA. Pour atteindre cet objectif, ils devraient s'entourer d'une équipe d'évaluation multidisciplinaire et consulter les représentants des intérêts concernés par le profilage, y compris les personnes profilées. Ce processus d'évaluation devrait être mené par des personnes dotées des qualifications professionnelles et des connaissances adéquates pour apprécier les différents impacts, y compris dans leurs dimensions juridique, sociale, éthique et technique ».

[42] Groupe d'experts de haut niveau sur l'intelligence artificielle, Lignes directrices en matière d'éthique pour une IA digne de confiance, avril 2020, disponible sur le site : https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[43] « *The Guidelines put forward a set of 7 key requirements that AI systems should meet in order to be deemed trustworthy: Human agency and oversight; Technical Robustness and safety; Privacy and data governance; Transparency; Diversity, non-discrimination and fairness; Societal and environmental well-being; Accountability* ».

[44] Soit, sous forme d'acronyme, la ALTAI paru le 17 juillet 2020, disponible à l'adresse suivante : https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.

[45] Proposition de règlement du Parlement européen et du Conseil relatif à un marché unique des services numériques (Loi sur les services numériques) et modification de la directive 2000/31/CE, COM(2020) 825 finale, Bruxelles 15 décembre 2020, disponible en ligne sur https://ec.europa.eu/digital-single-market/en/digital-services-act-package.

[46] Article 26 : « *Les très grandes plateformes en ligne recensent, analysent et évaluent, à compter de la date d'application visée au second alinéa de l'article 25, paragraphe 4, puis au moins une fois par an, tout risque systémique important trouvant son origine dans le fonctionnement et l'utilisation faite de leurs services au sein de l'Union…* ».

[47] Dans le même sens, C. Castets-Renard, « Accountability of Algorithms in the GDPR and beyond: A European Legal Framework on Automated Decision-Making » (May 20, 2019), *Fordham Intellectual Property, Media & Entertainment Law Journal*, https://ssrn.com/abstract=3391266 ou http://dx.doi.org/10.2139/ssrn.3391266 ; Y. Meneteu, *L'intelligence artificielle en procès*, *op. cit.*, pp. 366 et s. (cet auteur met en exergue certains principes qui devraient régir l'IA et en appelle à une convention-cadre internationale).

[48] J. Eynard, « Réflexions pour une intelligence artificielle digne de confiance », article à paraître, p. 6.

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021

de profilage utilisant l'IA, qui pour la plupart doivent être considérés à haut risque. S'impose ainsi, à travers les textes dits d'éthique de l'IA, la généralisation pour ces systèmes d'une procédure d'évaluation des risques que ces textes estiment devoir, en tout cas dans certains cas, être externe et facilitée par des systèmes de certification et de labellisation. La troisième est la méfiance vis-à-vis d'un *consentement individuel* répondant aux conditions du RGPD, comme base de licéité des systèmes de profilage. Nous plaidons pour des régimes d'exception en particulier lorsqu'il y a déséquilibre manifeste d'informations entre la personne concernée et le responsable du traitement ou au vu de l'impact économique et social lié au traitement de profilage généré[49]. La négociation collective ou la réglementation légale *a priori* de certaines applications comme la reconnaissance faciale ou l'utilisation de l'IA dans certains secteurs comme l'assurance ou l'octroi de crédit nous paraissent alors s'imposer.

22. Mais notre commentaire ne s'arrête pas là. Ce qui caractérise les enjeux de l'IA, c'est qu'ils débordent de loin les aspects de protection d'intérêts et de libertés individuels, ceux pour la protection desquels ont été adoptées les législations de protection des données. Les enjeux environnementaux, de justice sociale, de démocratie sont désormais au cœur des textes éthiques qui, à propos de l'IA, se succèdent dans les instances internationales. L'IA certes peut être un moyen de prévention et de lutte contre ces risques collectifs, il est également cause de leur aggravation. Que cela nécessite au-delà d'un PIA un « *Ethical Values Assessment* » nous paraît s'imposer. Reste à veiller à l'articulation entre ces deux types d'évaluation et faire en sorte que le second ne nuise pas au premier et ne prive nos autorités de protection des données de leur compétence en la matière. Nous plaidons pour une approche concertée entre les diverses autorités qui dans nos pays sont en charge des questions soulevées par les divers risques individuels et collectifs soulevés par l'IA et ses applications de profilage : respect des libertés et des droits fondamentaux : notamment des droits à la vie privée, à la dignité humaine et à la liberté d'expression ; respect des impératifs de justice sociale, de diversité culturelle et de démocratie. Nous prônons l'existence, à l'instar de pays proches et conformément aux vœux de la Commission européenne, d'un organe de coordination chargé d'une approche éthique de l'innovation que représentent les applications du « *machine learning* ». Il s'agit de construire, comme y appelle l'UIT, une « *AI for good* »[50], au service de l'humain et maîtrisée par lui.

[49] En particulier, le développement des systèmes de profilage par les *Tech Giants* (ou GAFAM) et les plateformes suscite l'inquiétude dans la mesure où outre la puissance économique qu'offrent les consortia qu'ils ont créés, leur rôle de *gatekeepers* autorise une collecte infinie de données.

[50] L'ITU a organisé en 2018 l'« *AI for Good Global Summit* ». Le prochain sera organisé à Genève en septembre de cette année. V. le site de l'ITU : https://www.itu.int/en/ITU-T/AI/2018/Pages/default.aspx. « *As the UN specialized agency for information and communication technologies, ITU is well placed to guide AI innovation towards the achievement of the UN Sustainable Development Goals. We are providing a neutral platform for international dialogue aimed at building a common understanding of the capabilities of emerging AI technologies* ».

Université de Namur - Bibliothèque de la Faculté de droit - On Campus / UNamur On Campus (138.48.8.152)
Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle
www.stradalex.eu - 28/09/2021