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

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

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

Poullet, Yves

Published in:
Un droit de l'intelligence artificielle : entre règles sectorielles et régime général

Publication date:
2023

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 2023, 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. Dans Un droit de l'intelligence artificielle : entre règles sectorielles et régime général: perspectives comparées. Bruylant, Bruxelles, p. 529-652.

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: 28. Apr. 2024

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 ?

YVES POULLET
PROFESSEUR ÉMÉRITE UNAMUR
PROFESSEUR ASSOCIÉ À L'UCLILLE
CO-PRÉSIDENT DU NADI
MEMBRE DE L'ACADÉMIE ROYALE DE BELGIQUE

RÉSUMÉ

En 2016, pour certains traitements « à risque élevé », le RGPD consacre, en ses articles 35 et suivants, l'obligation du ou des responsables de recourir à un PIA. Cette obligation s'inscrit dans une approche nouvelle de la réglementation de la protection des données : elle se fonde sur le principe de la responsabilité de ceux qui mettent en place des traitements, apparaît comme une forme nouvelle de corégulation ou de métarégulation, instille une approche d'une régulation fondée sur les risques et augure d'une démarche préventive plutôt que répressive de la protection des données. Cette « révolution » dans la réglementation des données est cependant loin d'être parfaitement dessinée et assumée par les dispositions précitées. La procédure d'évaluation instituée par le RGPD porte en germe les dispositions proposées par la Commission dans le cadre du futur *AI Act*, qui entend instaurer, de manière plus large et sans doute mieux précisée, une procédure d'*Ethical Values Impact Assessment*. Notre propos est d'esquisser une comparaison entre les deux régimes et les questions posées par leur coexistence, au moment où les applications de l'IA créent des risques nouveaux tant en matière de protection des données que de justice sociale, voire de démocratie.

BRUYLANT

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

1. Le PIA et ses origines[1] **–** La consécration du *Privacy Impact Assessment*, en abrégé PIA, comme élément majeur de protection des données, a une double origine outre-Atlantique à la fois tenant d'une approche réglementaire et à la fois traductrice d'une approche d'autorégulation. L'US *Privacy Act* de 1974[2] institue l'obligation pour toutes les administrations fédérales, et uniquement pour elles, de produire, lors de la création, de la modification ou du partage de traitements, un rapport d'évaluation des risques portant sur la protection des données qui, par ailleurs, fait l'objet d'une publication[3]. Dans le secteur privé, cette évaluation a été soulignée par nombre de codes de conduite et autres instruments d'autorégulation comme une conséquence logique du principe d'« *accountability* »[4], cher à l'approche autoréglementaire et consacré depuis 1980 par les lignes directrices de l'OCDE[5]. On ajoute qu'en 2013, lors de la révision des « Lignes directrices de l'OCDE

1. Sur les origines du PIA, voy. part. R. CLARKE, « Privacy Impact Assessment : its origins and development », *CL&SR*, 2014, pp. 123 et s. L'auteur analyse, de manière complète, l'émergence du concept et sa réception dans différents pays (comme les États-Unis, l'Australie, le Canada et la Nouvelle Zélande).

2. Privacy Act of 1974, as amended, 5 U.S.C. § 552a. Pour un commentaire complet de la législation, voy. l'« Overview of the Privacy Act of 1974 » (Privacy Act of 1974 [justice.gov]). On note que, depuis 1974, la Section 208 du E-Government Act of 2002 a complété les dispositions du privacy act : le texte impose aux administrations de mener des PIA pour leurs systèmes d'information et base de données. Sauf exceptions (secrets commerciaux, informations classifiées ou autres motifs d'intérêt public), les PIA doivent être rendus publics (à ce sujet, voy. la liste des PIA approuvés sur le site consacré au Privacy Act, Office of Privacy and Open Government, U.S. Department of Commerce, disponible en ligne à l'adresse https://www.osec.doc.gov/opog/PrivacyAct/PrivacyAct_SORNs.html.

3. « *A PIA must be conducted before: Developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government). A PIA must be updated to reflect changed information collection authorities, business processes, or other factors affecting the collection and handling of information in identifiable form, in addition to where a system change creates new privacy risks, such as: Conversions; Anonymous to Non-Anonymous; Significant System Management Changes (notably by using new technologies); Significant Merging New Public Access – when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public; Commercial Sources; New Interagency Uses; Internal Flow or Collection (significant new uses, disclosures or incorporation of information into the system); Alteration in Character of Data (e.g. by addition of health or financial information)* ».

4. Selon la Commission nationale de l'informatique et des libertés en France, « l'*accountability* désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de *démontrer le respect des règles relatives à la protection des données* ».

5. On note que les Lignes directrices de l'OCDE (1980), qui prônent l'autoréglementation en matière de protection des données, ont consacré ce principe : « *a data controller should be accountable for complying with measures which give effect to the principles stated above* ». Voy. égal. le même principe défendu par la Canadian Standards Association Privacy Charter (1995) et par l'APEC Privacy Framework (2005) et les International Standards on Privacy Protection. Enfin, on se référera utilement aux *Guidelines for Privacy Impact Assessment* édictées par l'ISO (norme ISO/IEC 29134:2017 disponibles en ligne à l'adresse https://iso.org/obp/UI:#iso:std:iso-iec:29134:ed-1:v1;en.

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

relatives à la protection des données et aux flux transfrontières », l'OCDE a précisé ce principe en réclamant aux entreprises un *Privacy Management Program* (en abrégé PMP) : « *PMPs need to be tailored to the structure, scale, volume and sensitivity of the controller's operations, integrated into the controller's governance structure and routinely reviewed and updated and that ssential elements of PMPs include appropriate safeguards based on privacy risk assessments. The need for mechanisms ensuring that third parties maintain appropriate safeguards when processing data on behalf of the controller and plans for responding to incidents and inquiries as well as internal oversight mechanismes were codified* ».

En écho à ce principe, la convention du Conseil de l'Europe n° 108+[6] étend l'obligation d'évaluation « de l'impact potentiel » sur les droits et libertés fondamentales à tout traitement de données envisagé. On note que cette disposition ne précise pas le comment de cette procédure et ne distingue pas les traitements ni suivant les risques y liés, ni suivant la nature publique ou privée de son responsable. Le choix du RGPD[7] d'imposer cette évaluation, tant aux secteurs public que privé, s'inspire de ce principe d'« *accountability* »[8], que l'article 5.2[9] introduit parmi les principes mêmes de légitimité de tout traitement. Il est certain que le succès, en particulier aux États-Unis, de cet instrument est à la base de sa consécration par le RGPD. Par ailleurs, le RGPD envisage de réserver cette obligation aux seuls traitements à risque élevé, fixe les critères à suivre pour la détermination de tels risques et aborde quelques précisions sur la procédure à suivre. Après avoir résumé l'essentiel des dispositions du RGPD relatives à ce *Privacy Impact Assessment*, nous aborderons la façon dont la récente proposition de la Commission européenne relative à un règlement sur l'intelligence artificielle[10], à propos d'applications relevant de l'utilisation de ces technologies et traitant de données à caractère

6. L'article 10.2 de la Convention 108+ énonce : « Chaque Partie prévoit que les responsables du traitement, ainsi que, le cas échéant, les sous-traitants, doivent procéder, préalablement au commencement de tout traitement, à l'examen de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des personnes concernées, et qu'ils doivent concevoir le traitement de données de manière à prévenir ou à minimiser les risques d'atteinte à ces droits et libertés fondamentales ».

7. La directive 2016/680 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 matière d'exécution de sanctions pénales prévoit de même à l'article 27, cette analyse d'impact.

8. À cet égard, parmi d'autres auteurs, voy. N. Metallinos, « Le principe d'*accountability* : des formalités préalables aux études d'impact sur la vie privée », *Comm. comm. electr.*, 2018, dossier 11.

9. « Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté. »

10. Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, SEC(2021) 167 final – SWD(2021) 84 final – SWD(2021) 85 final, 21 avril 2021, COM(2021) 206 final, disponible en ligne à l'adresse https://

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

personnel, aborde de manière différente et élargie cette obligation d'évaluation, sans qu'à la lecture du texte, les relations entre la proposition et le RGPD et en particulier la complémentarité des deux modes d'évaluation proposés ne soient totalement claires : « *The development and use of AI systems will in many cases involve the processing of personal data. Ensuring clarity of the relationship of this Proposal to the existing EU legislation on data protection is of utmost importance. The Proposal is without prejudice and complements the GDPR, the EUDPR and the LED. While the recitals of the Proposal clarify that the use of AI systems should still comply with data protection law, the EDPB and EDPS strongly recommend clarifying in Article 1 of the Proposal that the Union's legislation for the protection of personal data, in particular the GDPR, EUDPR, ePrivacy Directive*[11] *and the LED*[12]*, shall apply to any processing of personal data falling within the scope of the Proposal. A corresponding recital should equally clarify that the Proposal does not seek to affect the application of existing EU laws governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments* »[13].

La raison de cette double analyse et de la confrontation des procédures d'évaluation que ces textes mettent en place est évidente : l'utilisation de technologies d'IA pour le traitement de données à caractère personnel se multiplie, qu'il s'agisse des systèmes de reconnaissance faciale, voire d'émotions, des systèmes de recommandations individualisées de produits ou de messages, de lutte contre le terrorisme, de recherche en matière de santé, de robots aide-soignant… Les raisons sont multiples : les systèmes d'IA, en particulier celui de *machine learning*, permettent aux entreprises, administrations, voire aux citoyens, d'optimiser les décisions à prendre quand ces dernières ne sont pas le fait direct de ces systèmes. Chacun se plaît à louer l'objectivité de leur fonctionnement fondé sur des données collectées en quantité souvent au cœur de notre vie quotidienne. Enfin, ces systèmes permettent non seulement un

eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN, en abrégé « Artificial intelligence Act ».

11. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2006/24/EC and Directive 2009/136/EC.

12. 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, *JOUE*, L 119 du 4 mai 2016, pp. 89-131.

13. EDPB/EDPS, Joint opinion 5/2021 on the Proposal, n° 15.

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

regard sur le passé des personnes, mais prédisent le futur de leur capacité intellectuelle, de leur dangerosité, de leur capacité de crédit[14], de leurs choix politiques, de leur santé. La considération des performances inédites de tels systèmes ne peut ignorer les risques y liés[15]. L'opacité de leur fonctionnement jointe à l'imprévisibilité de leur évolution, la présence de possibles biais et erreurs dans leur conception, le renforcement sans précédent du déséquilibre informationnel entre ceux qui utilisent de tels systèmes et ceux auxquels on oppose la vérité sortie de tels systèmes, autant de sources de risques pour nos libertés individuelles qui s'ajoutent à ceux liés aux traitements traditionnels de données à caractère personnel. En d'autres termes, il est certain que l'IA met au défi l'adéquation du RGPD à assurer notre protection des données et, par-là, nos libertés individuelles. Par ailleurs, le règlement et nombre de textes d'organisations publiques internationales tant publics que privés[16] obligent à s'interroger sur l'approche nouvelle des risques liés à l'IA, bien plus large que celle du RGPD centrée sur la seule protection des données[17].

2. Les articles 35 et suivants du RGPD en quelques lignes – Il ne s'agit pas ici de nous livrer à une analyse exhaustive des deux articles du RGPD qui introduisent le PIA dans l'arsenal des dispositions de protection des données. Le Groupe de l'article 29 a proposé cette analyse systématique des dispositions[18]

14. À ce propos, les réflexions reprises au considérant n° 37 de la proposition AI Act : « les systèmes d'IA utilisés pour évaluer la note de crédit ou la solvabilité des personnes physiques devraient être classés en tant que systèmes d'IA à haut risque, car ils déterminent l'accès de ces personnes à des ressources financières ou à des services essentiels tels que le logement, l'électricité et les services de télécommunication. Les systèmes d'IA utilisés à cette fin peuvent conduire à la discrimination à l'égard de personnes ou de groupes et perpétuer des schémas historiques de discrimination, par exemple fondés sur les origines raciales ou ethniques, les handicaps, l'âge ou l'orientation sexuelle, ou créer de nouvelles formes d'incidences discriminatoires ».

15. Le « White paper » de la Commission (Commission européenne, *White Paper on Artificial Intelligence. A European approach to excellence and trust*, Bruxelles 19 février 2020, COM(2020) 65 final, qui a précédé les initiatives de la Commission relatives à la réglementation de l'IA, mettait déjà en évidence les risques inhérents à tout système IA : « *The specific characteristics of many AI technologies, including opacity ('black box-effect'), complexity, unpredictability and partially autonomous behavior, may make it hard to verify compliance with, and may hamper the effective enforcement of, rules of existing EU law meant to protect fundamental rights. Enforcement authorities and affected persons might lack the means to verify how a given decision made with the involvement of AI was taken and, therefore, whether the relevant rules were respected. Individuals and legal entities may face difficulties with effective access to justice in situations where such decisions may negatively affect them* ».

16. Y. Poullet, « About some international documents relating to the ethics of Artificial Intelligence – Some insights », in H. Jacquemin (coord.), *Time to reshape the Digital Society*, Cahier du CRIDS, 2021, pp. 523 et s.

17. Le propos de ce paragraphe renvoie à notre ouvrage : *Le RGPD au défi de l'intelligence artificielle*, Cahier du CRIDS, n° 48, Bruxelles, Larcier, 2021 ; voy. aussi parmi une nombreuse littérature, Y. Meneceur, *L'intelligence artificielle en procès*, coll. Macro Droit – Micro Droit, Bruxelles, Bruylant, 2020.

18. G.29, Lignes directrices du 4 octobre 2017 concernant l'analyse d'impact relative à la protection des données et la manière de déterminer si le traitement « est susceptible d'engendrer un risque élevé » aux fins du Règlement 2016/679, WP.248, Rev. 01, confirmées par le CEPD,

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

et relevé les points essentiels à notre propos. L'analyse d'impact est imposée (art. 35.1.) 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 ». La priorité accordée au critère « du recours aux nouvelles technologies »[19] mérite d'être soulignée. Elle indique clairement que les auteurs du RGPD étaient d'emblée conscients de la nécessité d'une évaluation des applications générées par les technologies alors émergentes, telles l'IA, comme la reconnaissance faciale, et largement utilisées en matière de profilage. L'article 35.3 décrit un certain nombre de traitements pour lesquels l'analyse est requise et, au-delà, délègue, aux autorités nationales de protection sous le contrôle et la coordination du CEPD, le soin de fixer et publier une liste positive et négative des traitements soumis ou non à l'obligation[20]. On ajoute que les listes retenues par le RGPD et par les autorités de contrôle ne sont pas exhaustives. Comme le note le Groupe 29[21], « d'autres opérations pouvant bien évidemment présenter un risque aussi élevé ».

Le paragraphe 7 de l'article 35 décrit le contenu minimum de l'analyse[22]. La procédure d'analyse est peu décrite[23]. Elle doit impliquer le détaché à la protection des données et, le cas échéant, requiert l'avis des personnes concernées ou de leurs représentants. Au cas où l'analyse d'impact révèle un risque élevé « si le responsable ne prenait pas de mesures pour atténuer

successeur du Groupe de l'article 29. Le lecteur se référera également utilement aux commentaires du RGPD, ainsi, celui publié par Th. DOUVILLE, *Droit des données à caractère personnel*, Gualino, Lextenso, 2021, pp. 227 et s.

19. Souligné par le considérant n° 91. Voy. aussi les lignes directrices du G.29 (p. 12) qui précise que, dans ce cas, le risque est accru du fait que ces nouvelles technologies de collecte (internet des objets) et d'utilisation des données peuvent avoir des conséquences personnelles ou sociales inconnues.

20. Ainsi, la CNIL a établi deux listes (CNIL, délibération n° 2018-326 portant adoption de lignes directrices sur les analyses d'impact relatives à la protection des données prévues par le RGPD). Sur ces deux listes, voy. le commentaire de A. DEBET et N. METTALINOS in *Comm. Comm electr.*, janvier 2019. Ces lignes directrices ont fait l'objet, le 25 septembre 2018, de l'avis 9/2018 du CEPD.

21. G.29, Lignes directrices, préc., p. 10. Le G.29 énumère pas moins de 9 critères qui devraient être pris en compte dans cette évaluation du risque et considère que la présence de deux de ces critères doit aboutir à la conclusion de la présence d'un risque élevé. Sur ce point, les commentaires de N. METALLINOS, « Consécration du rôle central des études d'impact sur la vie privée », *Comm. comm. électr.*, 2017, comm. 57.

22. Soit les points suivants : « a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ; b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ; c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1 ; et d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées ».

23. R. PERRAY, « Les outils de la conformité au RGPD : des outils de valorisation », *RAE*, dossier spécial (C. CASTETS-RENARD, éd.), 2021, p. 44.

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

le risque », l'article 36 enjoint au responsable de consulter préalablement l'autorité de contrôle qui, le cas échéant, réagira par un avis motivé, tantôt en dénonçant la violation légale, tantôt en estimant que le risque a été mal identifié ou insuffisamment couvert. On note que c'est au responsable de traitement de décider si oui ou non il consultera l'autorité de contrôle et on peut dès lors craindre qu'il n'interprète de manière restrictive les conditions du recours à l'avis de cette dernière. Enfin, il est demandé (art. 35.11) au responsable du traitement de vérifier si le traitement est effectué en accord avec les résultats de l'analyse « au moins quand il se produit une modification du risque présenté par les opérations de traitement ».

3. Au-delà du *Privacy Impact Assessment*, la proposition de règlement sur l'intelligence artificielle – Le 21 avril 2021, la Commission publiait sa proposition de règlement sur l'IA : en abrégé l'*AI Act*[24]. Sans doute, ne s'agit-il pas, avec cette proposition, d'affronter une thématique comme c'est le cas du RGPD, à savoir la protection des données à caractère personnel, mais bien d'encadrer la mise sur le marché de produits ou services à raison des risques encourus par les individus, les groupes sociaux, voire la société. On ajoute que ces produits et services utiliseront bien souvent des données à caractère personnel, ce qui implique la référence au RGPD. Par ailleurs, l'approche par les risques, centrale dans la justification des PIA, est omniprésente dans la proposition et la nécessité d'obliger ceux qui conçoivent, mettent sur le marché ou utilisent de tels produits ou services, à évaluer et, si possible, de réduire ces risques répond à la même justification d'*accountability*.

L'*AI Act* repose sur une réglementation à géométrie variable suivant le degré de risques présentés par les applications technologiques. Ainsi, le texte interdit ce qu'il considère comme des pratiques illégales de l'IA[25] (art. 5) ; soumet à des obligations spécifiques de transparence pour certaines applications

24. Cette proposition s'appuie sur divers documents : en particulier, le livre blanc (*White paper on Artificial Intelligence – A European approach to excellence and trust*, COM(2020) 65 final, 8), février 2020, exprime la stratégie européenne de « troisième voie » d'une IA d'excellence et de confiance et les travaux de l'HLGE on AI (High Level Group of experts on AI), notamment sa publication des *Lignes directrices en matière d'éthique pour une IA digne de confiance* (publiée le 8 avril 2019), texte disponible en ligne à l'adresse Ethics guidelines for trustworthy AI – Publications Office of the EU (europa.eu) – https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. 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. Sur les méthodes d'évaluation et les critères à prendre en compte, voy. le site de présentation d'Altai (Assessment List fot Trustworthy AI) : https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence.

25. Ainsi, les systèmes de manipulation par messages subliminaux, l'exploitation des vulnérabilités, l'utilisation par le secteur public de systèmes de « *social ranking* » entraînant de potentielles discriminations entre personnes ou groupes, de systèmes biométriques fonctionnant

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

cachées, en particulier la reconnaissance par l'IA des émotions ; impose aux applications dites « à haut risque » à un système d'évaluation, de contrôle et de gestion (art. 6.2) et, enfin, abandonne à l'autoréglementation du marché les autres applications présentant un risque minime. Nous n'évoquerons[26] ici que les dispositions spécifiques relatives aux systèmes à haut risque dans la mesure où le régime d'évaluation proposé permet une comparaison utile avec celui mis en place par le RGPD. Cette catégorie est large : il s'agit, d'une part (art. 6.1.), des systèmes d'IA destinés à être utilisés à part entière ou comme composants de sécurité de produits et soumis par un règlement ou directive existant à une évaluation de conformité *ex ante* (ainsi, les dispositifs médicaux, les produits financiers et d'assurance, les dispositifs embarqués dans les jeux ou les automoteurs…)[27], et, d'autre part (art. 6.2.), de systèmes d'IA ayant principalement des incidences sur les droits fondamentaux et explicitement énumérés[28] à l'annexe III (identification biométrique, accès et évaluation dans le secteur de l'éducation, évaluation des candidats lors d'une procédure de recrutement, police, justice…). On note que nombre de ces systèmes à haut risque concernent des traitements de données à caractère personnel soumis dès lors également au RGPD.

Les fournisseurs (*providers*) de systèmes IA à haut risque se voient imposer de multiples devoirs (art. 16). De tels systèmes d'IA doivent en effet respecter certaines exigences et être l'objet d'une évaluation interne[29] de

en temps réel et à distance, placés dans des endroits publics (par ex., des systèmes de reconnaissance faciale…).

26. Pour un exposé plus complet, voy. Y. POULLET, « Vers un droit européen de l'intelligence artificielle », *JDE*, janvier 2022, à paraître, et les références y citées.

27. Les nombreux textes réglementaires, qui pourraient être à l'origine d'une telle obligation de sécurité et donc soumis aux exigences de l'AI Act s'ils utilisent un système IA, sont listés à l'annexe I. Ainsi un robot médical, les dispositifs des voitures dites intelligentes, les systèmes de *credit rating* utilisés par les organismes financiers seront désormais soumis aux exigences du règlement sur les dispositifs médicaux de 2017 ou du règlement de 2018 sur les véhicules automoteurs, mais en outre à l'obligation d'évaluation prévue par l'AI Act.

28. L'annexe III reprend la liste susceptible d'évolution de huit types de systèmes à haut risque : systèmes biométriques d'identification (reconnaissance faciale ; utilisation des empreintes digitales, etc.) systèmes de gestion des infrastructures critiques (trafic routier, infrastructures de transport de gaz, électricité…) ; applications dans le secteur de l'éducation et de la formation (systèmes d'accès et d'évaluation des étudiants) ; applications en matière d'emploi (recrutement, contrôle et évaluation du personnel) ; applications en ce qui concerne l'accès ou la jouissance de services publics (en particulier les systèmes d'assistance) ou de services privés (évaluation de la valeur de crédit) essentiels (priorisation de l'accès à des systèmes de santé ou de secours) ; systèmes utilisés par les forces de l'ordre (évaluation de la dangerosité des personnes ; fiabilité des moyens de preuve, détection des émotions…) ; systèmes utilisés en matière de migration ou de contrôle des frontières ; systèmes d'administration de la justice (recherche et interprétation des faits ou interprétation et application de la loi). La liste peut être modifiée par la Commission (art. 7).

29. Sauf exception où c'est l'autorité dite « notifiante » qui vérifiera la conformité (art. 43). On note qu'en matière de systèmes d'IA de recommandations publicitaires ou de contenus utilisés par les très larges plateformes d'information et de communication, la proposition de Digital Service

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

conformité *ex ante*. La proposition impose l'établissement, la mise en œuvre, la documentation et la maintenance d'un système de gestion des risques (art. 9). Elle oblige au suivi de bonnes pratiques en matière d'évaluation des systèmes, en particulier l'utilisation d'ensembles de données répondant à différents critères de qualité (représentatifs, non biaisés, adaptés aux spécificités géographiques ou comportementales, etc.). L'article 10 mentionne divers devoirs liés à la gouvernance des données, ainsi le *testing* et la validation des choix de *design* et des données prises en compte, l'examen des biais possibles et, compte tenu de leur finalité, l'obtention d'un niveau approprié d'exactitude, de robustesse, de cybersécurité et de cohérence. On ajoute l'exigence d'une documentation technique avant la mise sur le marché ou la mise en service et son maintien, documentation par ailleurs détaillée dans son contenu et son format par l'annexe IV de la proposition (art. 11 et 18), tout en regrettant que la transparence du fonctionnement du système ainsi assurée ne concerne que l'utilisateur professionnel du système et non l'utilisateur final, citoyen ou entreprise qui, en définitive, se verra adresser les résultats de ce fonctionnement. La capacité d'enregistrement automatique d'événements (« journaux ») pendant le fonctionnement des systèmes d'IA (art. 12 et 20) doit être assurée. L'assurance d'un fonctionnement suffisamment transparent doit permettre aux utilisateurs d'interpréter les résultats du système et de les utiliser de manière appropriée. Enfin, la supervision effective par des personnes physiques pendant la période d'utilisation du système d'IA (*human oversight*)[30] est requise. Le projet mentionne le devoir de coopération avec les autorités nationales compétentes y compris en fournissant l'accès aux systèmes et à leur documentation.

4. La procédure d'évaluation selon l'*AI Act*[31] – L'article 19 dispose : « Les fournisseurs de systèmes d'IA à haut risque veillent à ce que leurs systèmes soient soumis à la procédure d'évaluation de la conformité applicable conformément à l'article 43, avant leur mise sur le marché ou leur mise en service. Lorsqu'il a été démontré, à la suite de cette évaluation de la conformité, que les systèmes d'IA satisfont aux exigences énoncées au chapitre 2 du présent titre, les fournisseurs établissent une déclaration UE de conformité conformément à l'article 48 et apposent le marquage "CE"

Act (en abrégé le DSA) impose cet audit externe, sa publication et le devoir des plateformes de se conformer aux recommandations de cet audit.

30. Art. 14.1 : « La conception et le développement des systèmes d'IA à haut risque permettent, notamment au moyen d'interfaces homme-machine appropriées, un contrôle effectif par des personnes physiques pendant la période d'utilisation du système d'IA ». On notera le flou d'une telle disposition.

31. À titre de comparaison, voy. le *Privacy Impact Assessment Guide*, publié par l'US Office of Personnel Management en avril 2010 et les annexes à remplir par les administrations tenues au PIA. Les rapports des administrations sont également publiés.

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

de conformité conformément à l'article 49 ». En particulier, un système de gestion de la qualité « garantissant le respect du règlement » doit être mis en place par les fournisseurs de systèmes à haut risque (art. 17). Pour la grande majorité des systèmes d'IA à haut risque, les fournisseurs (art. 23), ou utilisateurs suivent une procédure interne[32] d'évaluation de la conformité visée à l'annexe VI, qui ne prévoit pas d'intervention d'un organisme notifié[33]. Ils se devront de démontrer qu'ils ont suivi les normes harmonisées, lorsqu'elles existent[34]. Le règlement prévoit que certains systèmes à haut risque doivent faire l'objet d'un contrôle de conformité par les organismes notifiés désignés par l'autorité notifiante et se verront délivrer par ce dernier, « après information donnée, conformément à l'article 46.3, aux autres organismes notifiés accomplissant des activités similaires », un certificat conformément à la procédure de l'annexe VII[35]. Une base de données répertoriant les systèmes à haut risque listés par l'annexe III sera créée. On ajoute les obligations pour les fournisseurs de mise à jour et de notification des incidents graves et gérée par la Commission (art. 60). On note l'absence d'obligation de nommer un « *compliance officer* », comme c'est le cas en

32. Sauf quelques exceptions listées à l'annexe VII. À cet égard, les critiques adressées par un collectif d'auteurs qui soulignent le besoin d'étendre l'audit externe par des organismes agréés à d'autres systèmes IA à haut risque : « *Expand the list of high-risk systems which are subject to* prior independent conformity *assessment control. This should particularly be considered for AI systems that are used in contexts of asymmetry of power (such as, for instance, migration management and law enforcement), systems used for the biometric categorisation of individuals (which are currently not listed in Annex III), and systems relying on unscientific methods (such as polygraphs and emotion recognition systems, regardless of their deployment by a private or public actor)* » (N. SMUHA, E. AHMED-RENGERS, A. HARKENS, W. LI, J. MACLAREN, R. PISELLI et K. YEUNG, « How the EU can achieve Legally Trustworthy AI : A Response to the European Commission's Proposal for an Artificial Intelligence Act ? », Leads Lab @ University of Birmingham, 5 août 2021, p. 3 et développé pp. 48 et s., texte disponible en ligne à l'adresse https://ssrn.com/abstract=3899991).

33. « Chaque État membre désigne ou établit une autorité notifiante chargée de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle (organismes notifiés) » (art. 30). Les conditions et la procédure de désignation des organismes notifiés par les autorités nationales dites notifiantes, de même que leurs compétences respectives, sont décrites aux articles 30 et s.

34. Art. 40 : « Les systèmes d'IA à haut risque conformes à des normes harmonisées ou à des parties de normes harmonisées dont les références ont été publiées au *Journal officiel de l'Union européenne* sont présumés conformes aux exigences visées au chapitre 2 du présent titre, dans la mesure où celles-ci sont couvertes par ces normes ». On ajoute que la Commission peut, en cas d'absence de normes harmonisées, fixer elle-même après avis d'experts concernés et suivant une procédure fixée par le règlement (art. 74 et s.) la liste des « spécifications communes » nécessaires pour rencontrer les exigences du règlement (art. 41)

35. L'annexe VII prévoit le contrôle tant du système de gestion de la qualité que de la documentation. À propos du système de documentation, l'article 4.6 de l'annexe VII prévoit : « Lorsque le système d'IA est conforme aux exigences énoncées au titre III, chapitre 2, un certificat d'évaluation UE de la documentation technique est délivré par l'organisme notifié. L'attestation indique le nom et l'adresse du fournisseur, les conclusions de l'examen, les conditions (éventuelles) de sa validité et les données nécessaires à l'identification du système d'IA. Le certificat et ses annexes contiennent toutes les informations pertinentes pour permettre l'évaluation de la conformité du système d'IA et le contrôle du système d'IA pendant son utilisation, le cas échéant ».

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

matière de protection des données par la création d'un *Data Protection Officer*, dont le rôle en matière de PIA a été souligné. Certes, sur ce point, quelques exceptions existent[36]. Enfin, les autorités de surveillance du marché veillent au respect des exigences réglementaires et disposent pour ce faire d'un large accès aux données, à la documentation, voire au code source du système d'IA (art. 63 et s.). Elles peuvent, même pour un système conforme mais qui présenterait toutefois un risque pour la santé, la sécurité ou les droits fondamentaux, inviter « l'opérateur concerné à prendre toutes les mesures appropriées pour faire en sorte que le système d'IA concerné, une fois mis sur le marché ou mis en service, ne présente plus ce risque, ou pour le retirer du marché ou le rappeler dans un délai raisonnable, proportionné à la nature du risque, qu'elle prescrit ». Enfin, des sanctions sont possibles[37] sous forme d'amendes administratives (art. 71 et s.).

5. Une comparaison des deux régimes – les risques pris en compte – Les deux textes fondent clairement l'obligation d'évaluation sur une « *risk based approach* »[38]. L'article 35 du RGPD épingle la nature des risques qui déclenchent l'obligation du PIA. La notion de « risque élevé » renvoie aux traitements de données qui sont ou pourront être susceptibles d'avoir des incidences négatives sensibles pour les libertés et droits fondamentaux des personnes physiques. L'expression « susceptible de » ne signifie pas qu'il existe une lointaine possibilité d'incidence sensible. L'incidence sensible doit être plus probable qu'improbable. En revanche, cela signifie également qu'il n'est pas nécessaire que les personnes soient réellement affectées : la probabilité qu'elles soient sensiblement affectées suffit.

Il s'agit de « risques pour les droits et libertés des personnes concernées », en d'autres termes, ceux que le RGPD entend protéger suivant l'article 1.2. Pour Douville, mais son interprétation large est contestable, l'expression pourrait recouvrir « au-delà du droit au respect de la vie privée

36. On note (art. 15 règlement sur les dispositifs médicaux, *JOUE*, L 117/165 du 5 mai 2017) que « les fabricants disposent au sein de leur organisation d'au moins une personne chargée de veiller au respect de la réglementation possédant l'expertise requise dans le domaine des dispositifs médicaux ».

37. À noter : « Avant de prendre des décisions en vertu du présent article, le Contrôleur européen de la protection des données donne à l'institution, à l'agence ou à l'organe de l'Union faisant l'objet des procédures conduites par le Contrôleur européen de la protection des données la possibilité de faire connaître son point de vue sur l'éventuelle infraction. Le Contrôleur européen de la protection des données ne fonde ses décisions que sur les éléments et les circonstances au sujet desquels les parties concernées ont pu formuler des observations. Les éventuels plaignants sont étroitement associés à la procédure ». Il est à noter que seules les sanctions administratives sont énoncées explicitement sans que rien ne soit dit à propos d'autres mesures, telles que le retrait du produit du marché, l'injonction de conformité, etc.

38. Voy. art. 29 Data Protection Working Party, « *Statement on the role of a risk-based approach in data protection legal frameworks* », WP 218 du 30 mai 2014.

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

et à la protection des données à caractère personnel, la liberté de circulation, l'égalité et l'absence de discrimination, le droit à la santé, la liberté d'entreprendre ou le droit au respect des biens »[39]. On retrouve, à l'appui de cette interprétation large, la volonté de la Commission LIBE du Parlement d'apporter, lors de la discussion relative à l'adoption du RGPD, un amendement incluant spécifiquement les risques de discrimination dans le champ des risques créés par les traitements. Birnns[40] note que cet amendement a été rejeté par la suite, mais ajoute que le considérant 75 mentionne toujours ce risque. Bref, il est difficile de déterminer à l'heure actuelle si, dans le cadre de l'article 35 du RGPD, les questions d'égalité et de discrimination doivent être prises en considération lors de l'évaluation de la potentialité du risque lié au traitement de données. Cette question est importante, que l'on songe, par exemple, à l'utilisation de biométriques ou génétiques auxquels sont attachés autant des risques de libertés individuelles que de discrimination collective et qui sont considérés, dans le cadre de traitement par des systèmes d'IA, comme des systèmes à haut risque.

Précisément, la proposition relative aux systèmes d'IA élargit nettement le débat. Elle entend prendre en compte non seulement les risques encourus par 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[41]. 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 : « 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

39. Th. DOUVILLE, *Droit des données à caractère personnel*, *op. cit.*, n° 479, p. 228. On note que le Groupe dit de l'article 29, dans ses lignes directrices relatives au DPIA du 4 avril 2017 déjà citées, se réfère également, mais de manière incidente, aux risques de discrimination : « *As indicated in the Article 29 Data Protection Working Party Statement on the role of a risk-based approach in data protection legal frameworks, the reference to "the rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion* ».

40. R. BIRNNS, « Data Protection impact assessment : a meta regulatory approach », *Int. data &Privacy Law*, 2017, vol. 7, p. 28.

41. Sur la prise en compte de ces trois catégories de risques, présentes dans les textes internationaux en matière d'éthique de l'IA, voy. Y. POULLET, « About some international documents relating to the ethics of Artificial Intelligence – Some insights », in H. JACQUEMIN (dir.), *Time to reshape Information Society*, Actes du 40e anniversaire du CRIDS, Cahier du CRIDS, n° 52, pp. 501 et s.

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

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 ». En d'autres termes, la proposition de règlement de l'IA entend élargir le champ de l'évaluation au regard de celui auquel le RGPD se limitait. Selon le texte de la proposition, « elle complète ces actes [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… ».

L'*Ethical Values Assessment* proposé déborde dès lors celui imposé par le PIA 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

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

premier est l'ampleur du travail[42] et des compétences à réunir ou coordonner lorsqu'il s'agira de procéder à l'occasion, par exemple de l'évaluation d'applications destinées au pilotage de voitures intelligentes, de confronter 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 : le PIA est-il à mener distinctement des autres évaluations demain exigées par le règlement IA ? Sera-t-il ensuite ajouté ou intégré au rapport... ? ; troisièmement, on sait que le CEPD[43] a réclamé que les autorités de protection des données constituent les futures autorités de notification, en justifiant de leur compétence et de leur expérience en matière de PIA. Or, l'élargissement dont nous avons parlé infirme cette prétention. 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[44]. Ceci 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[45] qui coiffe l'ensemble des organismes nationaux de contrôle et de surveillance.

Quoi qu'il en soit, la nécessité 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 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 de rivalité entre instances.

42. 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.

43. EDPB/EDPS, *Joint opinion /2021 on the proposal for a regulation laying down harmonized rules on Artificial intelligence*, 18 juin 2021, en particulier la note 52.

44. Prenons l'hypothèse d'un système d'IA permettant le calcul des primes d'assurance-vie ou -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 de ces risques.

45. « Le Comité est composé des autorités de contrôle nationales, qui sont représentées par leur directeur ou un de leurs hauts fonctionnaires de niveau équivalent, et du Contrôleur européen de la protection des données. D'autres autorités nationales peuvent être invitées aux réunions, lorsque les questions examinées relèvent de leurs compétences » (art. 57).

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

6. Une approche préventive commune – L'approche par les risques induit une autre conséquence : elle justifie pleinement le passage d'une rédaction légale classique – fondée sur la définition de contenus comportementaux à respecter et, en cas de non-respect, sur la répression ou la sanction *a posteriori* des infractions à la réglementation – à une approche *a priori* fondée sur l'obligation d'évaluation des risques, soit la mise sur pied d'une procédure en la matière et du contrôle du respect de cette procédure. L'approche préventive fondée sur les risques semble être une caractéristique commune aux deux textes réglementaires étudiés. Le *Privacy Impact Assessment*, introduit par le RGPD, déplace ainsi le champ d'intervention de la réglementation vers une démarche préventive d'écartement ou de réduction des risques par la nécessité de mise sur pied d'une procédure d'évaluation dès la conception du traitement. La même idée traverse la proposition d'*AI Act* qui développe à loisir cette procédure, définissant ses étapes, son contenu, la gestion de qualité et des risques mise en place, etc. On soulignera cette manière de faire, certes, plus lourde administrativement et qui ne peut dès lors être justifiée que dans les cas de risques importants.

Les différences procédurales de l'évaluation sont certes remarquables. Les articles 35 et 36 du RGPD décrivent *a minima* les étapes et les acteurs à impliquer dans cette évaluation. Les critères d'appréciation du risque sont décrits de manière floue, même si les lignes directrices du Groupe 29 les ont quelque peu précisés[46]. À cet égard, l'*AI Act* est bien plus complet. La documentation à fournir (annexe VI), les informations nécessaires à l'enregistrement des systèmes IA auprès de la banque de données en vue d'établir leur conformité (annexe VIII) sont soigneusement détaillées et surtout le fournisseur se doit de mettre au point un système de gestion de qualité dont l'article 17[47] précise soigneusement les caractéristiques. Enfin, on notera la précision des critères d'appréciation du « haut risque » listés à l'article 6.2[48].

46. Voy. G.29, *Lignes directrices*, préc. *supra*, publiées le 4 octobre 2017, WP 248, pp. 11 et 12. Le groupe établit 9 critères. Cf. également sur cette base, les listes établies par les autorités nationales.

47. Art. 17 : « Les fournisseurs de systèmes d'IA à haut risque mettent en place un système de gestion de la qualité garantissant le respect du présent règlement. Ce système est documenté de manière méthodique et ordonnée sous la forme de politiques, de procédures et d'instructions écrites, et comprend au moins les aspects suivants […] ».

48. « Lorsqu'elle évalue, aux fins du paragraphe 1, si un système d'IA présente un risque de préjudice pour la santé et la sécurité ou un risque d'incidence négative sur les droits fondamentaux équivalent ou supérieur au risque de préjudice que présentent les systèmes d'IA à haut risque déjà visés à l'annexe III, la Commission tient compte des critères suivants : (a) la destination prévue du système d'IA ; (b) la mesure dans laquelle un système d'IA a été utilisé ou est susceptible de l'être ; (c) la mesure dans laquelle l'utilisation d'un système d'IA a déjà causé un préjudice à la santé et à la sécurité, a eu une incidence négative sur les droits fondamentaux ou a suscité de graves préoccupations quant à la matérialisation

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

Autre instrument préventif commun, l'apposition d'un certificat de conformité. Le RGPD, d'une part, et la proposition de règlement, d'autre part, mentionnent les certificats comme méthodes de vérification de conformité aux exigences réglementaires, mais leurs rôles respectifs sont cependant différents. Dans le cadre de l'article 42 du RGPD, la certification est volontaire, repose sur son octroi par des organismes de certification, dans le cadre de procédures et sur la base de critères définis par l'autorité de contrôle. Dans le cadre de la proposition, la certification de conformité par les autorités de notification est obligatoire pour les systèmes à haut risque et portent sur les éléments fondés sur des standards européens harmonisés (voy. le règlement n° 1025/2012)[49] et des spécifications établies par la Commission. Il ressort dès lors que la certification obtenue dans le cadre de la proposition ne correspond pas à celle spécifique sur la protection des données et obéit à d'autres objectifs[50]. On conçoit dès lors que le CEPD et l'EDPS dans leur opinion jointe (n° 23) réclament que le certificat de conformité des systèmes IA à haut risque couvre également la conformité aux

---

de ce préjudice ou de cette incidence négative, tel qu'il ressort des rapports ou allégations documentées soumis aux autorités nationales compétentes ; (d) l'ampleur potentielle d'un tel préjudice ou d'une telle incidence négative, notamment en ce qui concerne son intensité et sa capacité d'affecter plusieurs personnes ; (e) la mesure dans laquelle les personnes ayant potentiellement subi un préjudice ou une incidence négative dépendent des résultats obtenus au moyen d'un système d'IA, notamment parce qu'il n'est pas raisonnablement possible, pour des raisons pratiques ou juridiques, de s'affranchir de ces résultats ; (f) la mesure dans laquelle les personnes ayant potentiellement subi un préjudice ou une incidence négative se trouvent dans une situation vulnérable par rapport à l'utilisateur d'un système d'IA, notamment en raison d'un déséquilibre de pouvoir, de connaissances, de circonstances économiques ou sociales ou d'âge ; (g) la mesure dans laquelle les résultats obtenus au moyen d'un système d'IA sont facilement réversibles, les résultats ayant une incidence sur la santé ou la sécurité des personnes ne devant pas être considérés comme facilement réversibles ; (h) la mesure dans laquelle la législation existante de l'Union prévoit : i) des mesures de réparation efficaces en ce qui concerne les risques posés par un système d'IA, à l'exclusion des réclamations en dommages-intérêts ; ii) des mesures efficaces destinées à prévenir ou à réduire substantiellement ces risques. »

49. Règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 (*JOUE*, L 316/121 du 4 novembre 2012) relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil.

50. « *It is however not clear how certificates issued by notified bodies in accordance with the Proposal may interface with data protection certifications, seals and marks provided for by the GDPR, unlike what it is provided for other types of certifications (see Article 42(2) with regard to certifications issued under Regulation (EU) 2019/881)* (NdlA : il s'agit de la certification en matière de cybersécurité). *As far as high-risk AI systems are based on the processing of personal data or process personal data to fulfil their task, these misalignments may generate legal uncertainties for all concerned bodies, since they may lead to situations in which AI systems, certified under the Proposal and marked with a CE marking of conformity, once placed on the market or put into service, might be used in a way which is not compliant with the rules and principles of data protection* », EDPB/EDPS, *Joint opinion* (déjà citée), n° 74.

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

exigences du RGPD : « *To this end, the EDPB and the EDPS recommend including in Chapter 2 of Title III of the Proposal the requirement to ensure compliance with the GDPR and the EUDPR* ».

7. Des acteurs différents ? – En ce qui concerne les acteurs, on relève que l'obligation d'évaluation concerne, selon la terminologie du RGPD, le responsable du traitement, plus exceptionnellement le sous-traitant ; la proposition, suivant sa logique de considérer le système IA comme un produit que l'on met sur le marché, adresse cette obligation au « fournisseur » du « produit » IA. Cette notion est définie par l'article 3(2) comme suit : « "fournisseur", une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA en vue de le mettre sur le marché ou de le mettre en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit »[51]. Notons que le fournisseur est bien souvent une personne autre que le responsable du traitement : ainsi, lorsqu'une entreprise met au point, par exemple, un système de profilage de consommateurs, qu'elle implémente chez différents commerçants ou, autre exemple, un robot chirurgical qu'elle vend à des hôpitaux, elle ne peut être responsable de traitements que sur les données à caractère personnel qu'elle utiliserait dans le cadre des tests de mise au point du produit. Par contre, si elle est au sens de la proposition « fournisseur », son client, qui exploitera le système et traitera sans doute bien plus de données que l'entreprise qui a mis au point l'algorithme sera, selon la proposition de règlement, qualifiée d'utilisateur[52] et supportera une responsabilité bien moindre sur la base de cette dernière, tout en étant responsable au sens du RGPD et donc tenu, aux conditions de ce dernier, d'un PIA. Ensuite, on note qu'alors que le RGPD limite les devoirs liés au traitement aux seuls responsables et sous-traitants, l'*AI Act* envisage l'ensemble des acteurs[53] de la chaîne qui va depuis la conception du produit jusqu'à la fin de son utilisation et prescrit des obligations réciproques de certains acteurs vis-à-vis d'autres, en particulier en matière de documentation et de collaboration entre eux, ainsi du fournisseur de données vis-à-vis du fournisseur,

51. Cette définition laisse sur sa faim et apparaît comme lacunaire, ainsi au regard des systèmes d'IA développés par les pouvoirs publics, qui ne mettent pas à proprement parler sur le marché ces systèmes, ou par des organismes de recherche, qui développent des algorithmes d'IA en logiciel ouvert accessibles gratuitement, voire comme inadéquate lorsqu'une entreprise met au point avec de futurs potentiels utilisateurs (par ex., un organisme financier ou un groupe hospitalier) un système d'IA. Doit-on parler alors dans cette seconde hypothèse de fournisseurs conjoints ?

52. Art. 3 (4) : « "utilisateur", toute personne physique ou morale, autorité publique, agence ou autre organisme utilisant sous sa propre autorité un système d'IA, sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel ».

53. On retrouve ce même souci dans la récente recommandation du Conseil de l'Europe.

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

du fournisseur vis-à-vis de l'utilisateur[54] et inversement[55], etc. Cette tendance à créer des obligations entre les membres de la chaîne des acteurs dont la collaboration est nécessaire pour la réalisation d'un traitement se retrouve également en matière de protection des données, en particulier dans le texte de la recommandation récente du Conseil de l'Europe en matière de profilage[56].

8. De la corégulation à la responsabilité sociétale de certains acteurs – Quelques auteurs[57] voient dans la possibilité pour les entreprises ou administrations au terme d'une procédure interne d'évaluation le soin de fixer elles-mêmes la manière dont elles entendent répondre aux risques engendrés par les traitements qu'ils envisagent une forme de corégulation ou, pour être plus précis, comme le résultat d'une approche « *meta-regulatory* », définissant celle-ci comme « *any form of regulation (whether by tools of state law or other mechanisms) that regulates another form of regulation* », en l'occurrence « *the legal meta-regulation of internal corporate selfregulation* »[58]. Cette analyse que nous avons défendue à plusieurs reprises[59] est intéressante dans la mesure où elle renvoie à la responsabilité sociale de l'entreprise ou de l'administration, d'assumer dans un

54. Ainsi, l'article 21 : « Les fournisseurs de systèmes d'IA à haut risque qui considèrent ou ont des raisons de considérer qu'un système d'IA à haut risque qu'ils ont mis sur le marché ou mis en service n'est pas conforme au présent règlement prennent immédiatement les mesures correctives nécessaires pour le mettre en conformité, le retirer ou le rappeler, selon le cas. Ils informent les distributeurs du système d'IA à haut risque en question et, le cas échéant, le mandataire et les importateurs en conséquence ».

55. Art. 29, 2 et 4.

56. Recommandation CM/Rec(2021)8 du Comité des ministres aux États membres sur la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage, adoptée par le Comité des ministres le 3 novembre 2021. Ainsi, art. 3.12 : « Lorsqu'il(s) acquier(en)t des données ou des algorithmes d'un tiers, le ou les responsables du traitement devrai(en)t obtenir de ce tiers la documentation nécessaire à la vérification de la qualité des données et des algorithmes et de leur adéquation à la finalité poursuivie par le traitement ». Sur les arguments imposant de devoir créer des obligations vis-à-vis d'acteurs autres que les seuls responsables de traitement et sous-traitants, dans les textes relatifs à la protection des données, voy. B. FRENAY et Y. POULLET, « Profiling and Convention 108+: Report on developments after the adoption of Recommendation (2010)13 on profiling », Strasbourg, octobre 2020, T-PD(2019) 07 final, Comité consultatif de la Convention 108+, disponible en ligne à l'adresse https://rm.coe.int/t-pd-2019-7final-en-2757-5764-0706-1-2776-1394-9442-1/1680a0925c.

57. Voy. notamment D. WRIGHT, « Making Privacy Impact Assessment More Effective », *The Information Society*, 2013, vol. 29, n° 5, pp. 307-315, DOI : 10.1080/01972243.2013.825687 et réf. y citées ; R. BINNS, « Data Protection impact assessment. International Data Privacy assessments: a meta-regulatory approach », *International Data Privacy Law*, 2017, vol. 7, n° 1, pp. 29 et 30.

58. La définition est reprise de C.E. PARKER, *The Open Corporation Effective Self-Regulation and Democracy*, Cambridge, Cambridge University Press, 2002. L'auteur estime que l'autorégulation ne peut être prise au sérieux et être effective que si elle s'appuie sur une exigence et un cadre légaux.

59. Notamment in Y. POULLET, « Technologies de l'information et de la communication et 'co-régulation' : une nouvelle approche ? », in *Liber amicorum Michel Coipel*, Bruxelles, Kluwer, 2004, p. 173.

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

cadre réglementaire défini, par la procédure d'évaluation, les risques que son projet de système d'information fait courir, dans le cadre de l'article 35 du RGPD, aux personnes concernées et, dans le cadre de l'*AI Act*, au-delà des libertés individuelles, à certaines collectivités, à la justice sociale, à l'environnement, à la santé publique et à la démocratie[60].

La réponse de l'entité visée peut-être originale et innovante, ce qui importe c'est que la procédure ait été correctement menée. L'attention est mise autant sur la procédure que sur le résultat. Ceci nous amène à souligner quelques points déficients dans les deux textes analysés. Le premier point, au nom de la légitimité du document qui sera produit, exigerait en effet la participation de tous les représentants d'intérêts liés au fonctionnement envisagé du système. On sait que les premières versions du RGPD requerraient l'avis des personnes concernées lors de l'évaluation ; l'article 35.6 n'envisage désormais cet avis que « le cas échéant » et « sans préjudice de la protection des intérêts généraux ou commerciaux ou publics ou de la sécurité des opérations de traitement ». On déplore la même lacune dans le cadre de la proposition d'*AI Act*. Autre critique, l'absence de toute obligation de publier un rapport relatif à l'évaluation produite. Cette obligation, affirmée dans les premières versions du RGPD, a été abandonnée dans la version finale même si l'avis du Groupe 29 le recommande tout en soulignant que nombre d'objections liées au secret d'affaires et à la propriété intellectuelle peuvent s'y opposer. Dans le cadre de l'*AI Act*, l'annexe 5 relative à la déclaration de conformité ne mentionne pas l'obligation de déposer un rapport d'évaluation, même si la documentation obligatoire qui accompagne le produit fournit un certain nombre d'informations sur la qualité du produit, de l'évaluation à laquelle il a été procédé et des risques liés à son fonctionnement, mais ceux à l'attention des seuls utilisateurs professionnels qui mettront

60. « *Legal Trustworthiness requires the appropriate allocation of responsibility for harms and wrongs. A core function of modern legal systems is to provide a binding framework to enable peaceful social cooperation between strangers. The legal system achieves this inter alia by attributing legal responsibility to those whose activities produce 'other-regarding' harms or wrongs, whether intentional or otherwise, resulting in the imposition of either (or both) civil or criminal liability as appropriate. In this way, the law seeks to reduce and prevent harm to others, and to ensure appropriate redress where such adverse events occur. The law establishes and publicly promulgates legally binding rules which identify the scope and content of the rights and responsibilities of legal and other persons, thereby providing guidance to legal subjects so that they can alter their behaviour accordingly so as not to fall foul of the law's demands. This legal guidance function plays an important role in protecting the legal rights, interests and expectations of all members of the community against unlawful interference by others* » (N. Smuha, E. Ahmed-Rengers, A. Harkens, W. Li *et al.*, « How the EU can achieve Legally Trustworthy AI : A Response to the European Commission's Proposal for an Artificial Intelligence Act ? », Leads Lab @ University of Birmingham, 5 août 2021, p. 6, texte disponible en ligne à l'adresse https://ssrn.com/abstract=3899991).

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

en œuvre les applications permises par le système d'IA fourni. Ces deux points nous paraissent importants. Faute de participation de l'ensemble des *stakeholders* et de rapport mis à disposition du public, le résultat des procédures d'évaluation et de gestion de qualité au service de la protection des individus, des groupes et de la société risque d'être purement formel et d'aboutir à une conformité minimale. N'exige-t-on pas, au-delà d'une simple conformité, des traitements et des systèmes qui positivement poursuivent les valeurs éthiques et légales souhaitées ? Enfin, on note que, dans les deux textes, les autorités de surveillance ont le droit d'avoir accès à ce rapport d'évaluation et que son absence ou le non-respect de la procédure légale d'évaluation imposée peuvent être sanctionnés administrativement.

9. Des *Impact Assessments* particuliers à la création d'organes de coordination multidisciplinaire d'évaluation « éthique » des systèmes à risque élevé ou à haut risque – Au-delà des *Privacy Impact Assessment* et de l'*Ethical Values Impact Assessment* prônées par les deux textes à propos de traitements particuliers dits à risque élevé ou de systèmes d'IA dits à haut risque, ne faut-il pas prévoir une réflexion plus large lorsque des enjeux liés à une technologie émergente nécessite des choix sociétaires ? Ainsi, pour ne prendre que quelques exemples, la reconnaissance faciale, les systèmes de recommandation utilisés par les « *gatekeepers* » ou « *large platforms* », les traitements de données génétiques, l'assurance *one-to-one* ne peuvent voir leur validité décidée au hasard des différentes études d'impact menées à l'occasion des multiples projets à leur propos, mais doivent être l'objet d'une réflexion générale, voire, le cas échéant, de dispositions réglementaires précises. Ce besoin d'une discussion publique et d'une participation de la société civile sur les enjeux nous apparaît devoir être menées au sein d'une enceinte européenne ouverte de « *Data Ethics* ». Comme l'écrivent N. Smuha et consorts[61], dans un commentaire particulièrement critique de la proposition *AI Act*, la proposition présente une lacune importante, celle de l'absence de considération du droit à la participation des citoyens aux choix sociétaires que dessinent les avancées technologiques : « *The Proposal neglects to ensure meaningful transparency, accountability, and rights of public participation, thereby failing to provide adequate protection for democracy as the third pillar of Legally Trustworthy AI. In particular, 1. The public is not provided with consultation and participation rights regarding future revisions of the list of high-risk AI systems, nor regarding the determination of*

61. N. SMUHA *et al.*, « How the EU can achieve Legally Trustworthy AI : A Response to the European Commission's Proposal for an Artificial Intelligence Act ? », rapport préc., p. 3 et développé pp. 48 et s., texte disponible en ligne à l'adresse https://ssrn.com/abstract=3899991.

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

what constitutes an 'acceptable' residual risk in the context of high-risk AI systems. 2. The Proposal does not provide individuals with substantive rights not to be subjected to prohibited or otherwise noncompliant AI systems, illustrating the Proposal's complete lack of attention to 'ordinary people.' Nor are individuals granted meaningful information rights to enable them to form informed opinions and contest the development and deployment of controversial AI systems. 3. The Proposal does not provide for democratic input on the development of the technical standards crucial for the implementation of the proposed regulatory framework ».

Au-delà de la procédure d'évaluation interne aux entreprises ou administrations instaurées à propos d'applications précises, il serait utile, afin d'appuyer cette procédure interne, que l'Union européenne, si du moins elle suit les orientations du *White Paper* de janvier 2020 émis par la Commission, s'oriente, sur la base des modèles adoptés par des pays[62] comme le Danemark, l'Allemagne[63] ou le Royaume-Uni[64], vers la création

62. « *Member States are pointing at the current absence of a common European framework. The German Data Ethics Commission has called for a five-level risk-based system of regulation that would go from no regulation for the most innocuous AI systems to a complete ban for the most dangerous ones. Denmark has just launched the prototype of a Data Ethics Seal. Malta has introduced a voluntary certification system for AI* » (White paper, *op. cit.*, p. 11).

63. La Data Ethics Kommission fédérale a été mise en place le 5 septembre 2018. Elle est composée notamment de représentants de l'industrie, de représentants de l'APD. Elle a publié récemment (octobre 2019) un rapport important sur le développement des systèmes d'intelligence artificielle, accessible en ligne à l'adresse https://datenethikkommission.de/wp-content/uploads/191015_DEK_Gutachten_screen.pdf. Elle suggère une réglementation des systèmes d'IA basée sur la potentialité de dommages pour l'individu et la société : « *On this point, the central recommendation of the commission is to apply different regulations to autonomous systems based on a 5-point scale : 1. Systems with low potential harm such as drink dispensers should not be regulated. 2. Systems with some potential harm such as dynamic pricing in e-commerce should be lightly regulated and post-hoc controls should be set up. 3. Systems with regular or obvious potential harm such as personalized pricing should undergo an approval procedure associated to regular controls. 4. Systems with considerable potential harm, such as companies that have quasi-monopolies in credit scoring, should publish the details of their algorithms, including the factors used in the calculations and their weights, the data processed and an explanation of their inner logic. Controls should be possible via a real-time interface. 5. Systems with unwarranted potential harm such as autonomous weapons should be "fully or partially" forbidden.* » (résumé proposé par Algorithmwatch).

64. À propos de la « Data Ethics and innovation Authority » du Royaume-Uni, voy. le site de l'autorité : https://www.statisticsauthority.gov.uk/about-the-authority/committees/nsdec/data-ethics/ : « *The UK Statistics Authority aims to mobilise the power of data to meet the greater demand from policy makers and users for more timely, frequent, accurate and relevant statistics for the public good to help Britain make better decisions. This involves making better use of pre-existing administrative, real time and big data using innovative methods, to produce more frequent, timely and accurate statistics for the public good accounting for a wide variety of user needs. To ensure that this work is completed to the highest ethical standards the UK Statistics Authority has established a robust ethical*

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

d'un organe multidisciplinaire d'évaluation « éthique » des systèmes d'IA[65]. Le rôle de cette « Autorité pluridisciplinaire indépendante d'évaluation des risques liés à l'intelligence artificielle » serait de coordonner les activités des autorités nationales créées chacune dans leur domaine de compétences spécifiques (l'environnement, la sécurité, la justice sociale, la protection des consommateurs, la protection des données), afin de coordonner les compétences, règles et critères d'évaluation des systèmes IA[66]. Sans doute devrait-on dans cette perspective revoir la composition[67], le fonctionnement du Comité européen de l'intelligence artificielle institué par l'*AI Act* et, parmi ses compétences, développer celle mentionnée à l'article 56.2, (b), soit « coordonner les orientations et analyses de la Commission et des autorités de contrôle nationales et d'autres autorités compétentes sur les questions émergentes dans l'ensemble du marché intérieur en ce qui concerne les matières relevant du présent règlement, et de contribuer à ces orientations et analyses […] ».

governance structure to provide transparent and timely ethical advice to the National Statistician that the access, use and sharing of public data for research and statistical purposes is ethical and for the public good ».

65. Le Conseil de l'Europe s'oriente également vers une telle recommandation aux États membres. À cet égard, voy. le rapport sur l'intelligence artificielle remis par A. Mantelero au Conseil de l'Europe (ce rapport a servi de base à l'établissement des Lignes directrices adoptées par le Conseil de l'Europe en matière d'intelligence artificielle), en particulier les pages 16 et suivantes. L'auteur y souligne l'intérêt d'une approche à un niveau national en complément à la mise en place d'une procédure au niveau des entreprises. Cf. également le rapport Frenay-Poullet déjà cité en matière de profilage, de novembre 2019, au comité consultatif sur la Convention n° 108, préc., pp. 42 et s.

66. « *A European governance structure could have a variety of tasks, as a forum for a regular exchange of information and best practice, identifying emerging trends, advising on standardisation activity as well as on certification. It should also play a key role in facilitating the implementation of the legal framework, such as through issuing guidance, opinions and expertise. To that effect, it should rely on a network of national authorities, as well as sectorial networks and regulatory authorities, at national and EU level. Moreover, a committee of experts could provide assistance to the Commission* » (White paper, *op.cit.*, p. 24).

67. Cette autorité doit être ouverte aux différentes catégories de personnes intéressées par les applications de l'IA (représentants des travailleurs, des consommateurs, association de défense des libertés civiles, etc.). « *A European governance structure on AI in the form of a framework for cooperation of national competent authorities* (c'est-à-dire non seulement les autorités de protection des données mais celles de protection des consommateurs, de la concurrence, de l'audiovisuel, de l'égalité des chances…) *is necessary to avoid fragmentation of responsibilities, increase capacity in Member States, and make sure that Europe equips itself progressively with the capacity needed for testing and certification of AI-enabled products and services. In this context, it would be beneficial to support competent national authorities to enable them to fulfil their mandate where AI is used.* » […] « *The governance structure should guarantee maximum stakeholders participation. Stakeholders – consumer organization and social partners, businesses, researchers, and civil society organizations – should be consulted on the implementation and the further development of the framework* » (White Paper, *op. cit.*, p. 24).

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

Conclusions

10. L'évaluation des risques, une excellente initiative ? – Notre propos souligne l'intérêt de la procédure de *self assessement* mis en place par le RGPD. Elle se fonde à juste titre sur une approche basée sur les risques, ce qui permet une régulation asymétrique et mieux proportionnée en fonction des traitements et des technologies utilisés ; elle présuppose la responsabilisation des acteurs et les contraint à une évaluation et des mesures correctrices *a priori*[68]. Ceci dit, les deux propositions présentent des lacunes :

– elles reposent sur une autoévaluation interne des risques[69]. Sans doute est-il difficile, ne serait-ce que pour ne pas handicaper l'innovation européenne par des procédures d'audit externe[70] lourdes et peu appropriées, d'imposer le contrôle externe ? Ce choix aurait cependant nécessité des contrepoids aux décisions des responsables de traitement, premièrement, la participation des représentants des personnes demain soumises aux risques liés à la technologie, deuxièmement, la publication du rapport[71] et, troisièmement, la présence, comme l'exige

68. (La proposition constitue) « *a balanced and proportionate horizontal regulatory approach to AI that is limited to the minimum necessary requirements to address the risks and problems linked to AI, without unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market* » (Exposé des motifs de la proposition AI Act, préc., p. 3).

69. « *At the same time, the Proposal appears to leave an unduly large amount of discretion to the provider of the AI system as regards the execution of the risk management process. Article 9(4) leaves it up to the AI provider to determine which measures to take in order to ensure that any residual risk associated with each hazard as well as the overall residual risk of the high-risk AI systems is judged acceptable.* » « *This means that the decision about which risks are deemed "acceptable" is outsourced to the AI provider, who also seeks to put the system on the market or into service.* » (N. Smuha *et al.*, « How the EU can achieve Legally Trustworthy AI : A Response to the European Commission's Proposal for an Artificial Intelligence Act ? », rapport préc., pp. 48 et s.).

70. Comme cela serait imposé aux « *very large platforms* » d'information et de communication (c'est-à-dire aux réseaux sociaux et moteurs de recherche ayant une clientèle égale ou supérieure à 10 % de la population européenne) si la proposition dite *Digital Service Act* de la Commission européenne en cours de discussion. Selon cette proposition, ces plateformes auraient l'obligation d'effectuer des évaluations des risques dits systémiques provoqués par ou liés au fonctionnement et à l'utilisation de leurs services (art. 26) et de prendre des mesures raisonnables et efficaces visant à atténuer ces risques (art. 27). Elles doivent également se soumettre à des audits externes et indépendants (art. 28). Dans les cas où de très grandes plateformes en ligne utiliseraient des systèmes de recommandation (art. 29) ou afficheraient de la publicité en ligne sur leur interface en ligne (art. 30), elles font également l'objet d'obligations de transparence spécifiques. Elles accorderont l'accès à des données aux chercheurs pour comprendre comment évolue le risque en ligne ; elles nomment un ou plusieurs agents de conformité pour assurer le respect des obligations énoncées dans le règlement (art. 32) et se voient imposer des obligations spécifiques et supplémentaires en matière de rapports sur la transparence (art. 33).

71. On note que l'article 27 de la directive « Protection des données et Police » prévoit cette publication du rapport d'évaluation. « 1. Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et les libertés

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023

le RGPD, d'un « *compliant officer* ». Il est à craindre aussi non que les responsables ou les fournisseurs désireux d'éviter l'application des dispositions obligatoires pour les traitements à risque élevé ou les systèmes d'IA à haut risque plaideront l'inexistence de tels risques dans les cas concrets qui les occupent ou que les rapports se réduisant au résultat d'une obligation purement formelle.

L'interaction entre les deux types d'évaluation n'est pas évidente : la première repose sur le respect d'une réglementation dont le contenu et les principes sont particulièrement développés, mais qui laisse dans l'ombre nombre de détails sur la procédure à mettre en place ; la seconde apparaît centrée sur un produit mis sur le marché, détaille soigneusement la procédure et les outils de gestion de celle-ci, renvoie à des valeurs nombreuses à respecter, mais sans préciser les principes qu'impose le respect de ses valeurs. Sans doute, et la lecture des systèmes d'IA dits à haut risque, tels que listés à l'annexe 3 de la proposition de règlement *AI Act* l'atteste, les risques liés à la protection des données des futures applications d'IA constituent un élément majeur des préoccupations de la Commission et ont justifié de manière importante la proposition réglementaire. Il est clair que les systèmes d'IA accroissent les risques encourus par nos libertés individuelles, en particulier notre vie privée tant par leur opacité, tant par leurs capacités de traitement sans commune mesure avec celles traditionnelles, y compris celles de prédire nos vies, que par les risques de biais et d'erreurs. Tout cela justifie sans doute le rôle crucial des APD et du respect du RGPD. Faut-il pour autant réduire l'évaluation des systèmes d'IA à la prise en considération de ces seuls risques ? Nous ne le pensons pas et c'est sans doute un des mérites de l'*AI Act* d'avoir mis en valeur la nécessité de prise en considération d'autres risques cette fois collectifs ou de société et de plaider pour une collaboration plus étroite entre les divers organismes en charge de ces préoccupations plus larges que celles purement individuelles.

---

des personnes physiques, les États membres prévoient que le responsable du traitement effectue préalablement au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. 2. L'analyse visée au paragraphe 1 contient au moins une description générale des opérations de traitement envisagées, une évaluation des risques pour les droits et libertés des personnes concernées, les mesures envisagées pour faire face à ces risques, les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect de la présente directive, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes touchées ».

strada lex
UNamur On campus / quentin.houbion@unamur.be
L'analyse d'impact relative à la protection des données ou plutôt le privacy impact assessment, une révolution non sans lendema...
www.stradalex.com - 29/03/2023