The data protection impact assessment or rather the privacy impact assessment, a revolution with a future in the age of artificial intelligence ?

Poullet, Yves

Published in:
Artificial intelligence law

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

THE DATA PROTECTION IMPACT ASSESSMENT OR RATHER THE PRIVACY IMPACT ASSESSMENT, A REVOLUTION WITH A FUTURE IN THE AGE OF ARTIFICIAL INTELLIGENCE?

YVES POULLET
PROFESSOR EMERITUS, UNIVERSITY OF NAMUR
ASSOCIATE PROFESSOR UCLILLE
CO-CHAIR OF NADI
MEMBER OF ACADÉMIE ROYALE DE BELGIQUE

INTRODUCTION

1. The origins of the PIA[1]**.** The consecration of the "Privacy Impact Assessment," abbreviated to PIA, as a major element of data protection, has a double origin, across the Atlantic, both from a regulatory approach and from a self-regulatory approach. The US Privacy Act of 1974[2] instituted the obligation for all federal administrations, and only for them, to produce a risk assessment report on data protection when creating, modifying or sharing data, which is also published.[3] In the private sector, this assess-

1. On the origins of PIA, read in particular R. CLARKE, "Privacy Impact Assessment: its origins and development," 2014 *CL&SR*, pp. 123 et seq. The author provides a comprehensive analysis of the emergence of the concept and its reception in various countries (such as the United States, Australia, Canada and New Zealand).

2. Privacy Act of 1974, as amended, 5 U.S.C. § 552a. For a full commentary on the legislation, read the "Overview of the Privacy Act of 1974," (Privacy Act of 1974 (justice.gov)). Since 1974, Section 208 of the E-Government Act of 2002 has supplemented the provisions of the Privacy Act: the text requires administrations to conduct PIAs for their information systems and databases. Except for exceptions (trade secrets, classified information, or other reasons of public interest) the PIA must be made public (on this subject, see the list of approved PIAs on the site dedicated to the Privacy Act, Office of Privacy and Open Government, U.S. Department of Commerce, available at 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

ment has been emphasized by a number of codes of conduct and other self-regulatory instruments as a logical consequence of the "accountability" principle,[4] which is dear to the self-regulatory approach and has been enshrined since 1980 in the OECD guidelines.[5] It should be added that in 2013, during the revision of the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," the OECD clarified this principle by requiring companies to have a "Privacy Management Program" (PMP for short): "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 essential 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 mechanisms were codified."

Echoing this principle, the Council of Europe Convention No. 108+[6] extends the obligation to assess the "potential impact" on fundamental rights and freedoms to any planned data processing. We note that this provision does not specify how this procedure is to be carried out and does not distinguish between processing operations according to the risks involved or the public or private nature of the controller. The choice of the GDPR[7] to impose this evaluation, in both the public and private sectors, is inspired

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. According to la Commission Nationale de l'Informatique et des Libertés en France, "accountability" refers to the obligation for companies to implement internal mechanisms and procedures to demonstrate compliance with data protection rules (Our translation).

5. It is noted that the OECD Guidelines (1980), which advocate self-regulation in data protection, have enshrined this principle: "a data controller should be accountable for complying with measures which give effect to the principles stated above." See also the same principle defended by the Canadian Standards Association Privacy Charter (1995) and the APEC Privacy Framework (2005) and the International Standards on Privacy Protection. Finally, it is useful to refer to the "Guidelines for Privacy Impact Assessment," 2017, standard ISO/IEC 29134, available at https://iso.org/obp/UI:#iso:std:iso-iec:29134:ed-1:v1;en.

6. Art. 10.2 of Convention No. 108+ states: "Each Party shall provide that controllers and, where applicable, processors, examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimize the risk of interference with those rights and fundamental freedoms."

7. Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties likewise provides in Article 27 for this impact assessment.

by the principle of "accountability,"[8] which Article 5.2[9] introduces among the very principles of legitimacy of any processing. It is certain that the success of this instrument, particularly in the United States, was the basis for its consecration by the GDPR. On the other hand, it envisages reserving this obligation only to high-risk processing operations, sets out the criteria to be followed for determining such risks and addresses some details on the procedure to be followed. After summarizing the main provisions of the GDPR relating to this Privacy Impact Assessment, we will discuss the way in which the recent EU Commission's proposal for a regulation on artificial intelligence[10] (in short the AI Act) addresses this assessment obligation in a different and broader way, without referring, with regard to applications involving the use of these technologies and dealing with personal data, to the procedure of PIA set up by the GDPR but asserting the complementarity of the two assessment methods, even if the text of the AI Act is clear concerning in general the relationship with GDPR: "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

8. In this regard, among other authors, read N. METALLINOS, "Le principe d'a*ccountability*: des formalités préalables aux études d'impact sur la vie privée," 2018 *Comm. Comm. Electr.*, dossier 11.

9. "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1."

10. Proposal for a Regulation laying down harmonized rules on artificial intelligence and amending certain legislative acts of the Union (Artificial intelligence Act), 21 April 2021, COM(2021) 206 final, available at https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN. Our article refers to the original version provided by the Commission. A lot of debates at the EU Parliament and compromises at the Council have modified the original text but without important modifications, as regards our comment. The adoption of the final text is expected for the end of the year.

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 (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119*, *4.5.2016*, pp. 89-131.

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]

The reason for this double analysis and the confrontation of the evaluation procedures that these texts put in place is obvious: the use of AI technologies for the processing of personal data is multiplying, whether it is a question of facial or even emotional recognition systems, systems for individualized recommendations of products or messages, for the fight against terrorism, for health research, or for caretaker robots. There are many reasons for this: AI systems, especially machine learning systems, allow companies, administrations and even citizens to optimize the decisions to be made when these decisions are not made directly by these systems. Everyone likes to praise the objectivity of their operation based on data collected in quantity often at the heart of our daily life. Finally, these systems allow not only a look at the past of people but also predict the future of their intellectual capacity, their dangerousness, their credit capacity,[14] their political choices, their health. The consideration of the unprecedented performances of such systems cannot ignore the related risks.[15]

The opacity of the functioning of the AI machine learning system, particularly the so called "deep learning" applications combined with the unpredictability of their evolution, the presence of possible biases and errors in their design, the unprecedented reinforcement of the informational imbalance between those who use such systems and those who are opposed to

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

14. In this regard, the considerations set out in recital 37 of the AI Act proposal: "AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services. AI systems used for this purpose may lead to discrimination of persons or groups and perpetuate historical patterns of discrimination, for example based on racial or ethnic origins, disabilities, age, sexual orientation, or create new forms of discriminatory impacts."

15. The "White paper" of the Commission (European Commission, *White Paper on Artificial Intelligence*, *A European approach to excellence and trust*, Brussels, 19 February 2020, COM(2020) 65 final), which preceded the Commission's initiatives on AI regulation, already highlighted the risks inherent in any AI system : "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."

the truth coming out of such systems, all these are sources of risks for our individual liberties which are added to those linked to traditional processing of personal data. In other words, it is certain that AI challenges the adequacy of the GDPR to ensure our data protection and thereby our personal freedoms. Moreover, the regulation and a number of texts from international public organizations, both public and private,[16] force us to question the new approach to AI-related risks, which is much broader than the GDPR's focus on data protection of individuals alone.[17]

2. Articles 35 et seq. of the GDPR in a few lines. It is not our intention here to make an exhaustive analysis of the two articles of the GDPR that introduce the PIA into the arsenal of data protection provisions. The Article 29 Working Party has proposed this systematic analysis of the provisions[18] and noted the key points for our purposes. Impact assessment is required (Art. 35.1.) when the processing presents a "high risk," "in particular through the use of new technologies, and considering the nature, scope, context and purposes of the processing." The priority given to the "use of new technologies"[19] criterion is noteworthy. It clearly indicates that the authors of the GDPR were aware from the outset of the need to assess the applications generated by the then emerging technologies, such as AI, facial recognition and widely used profiling. Article 35.3 describes a number of processing operations for which analysis is required and, beyond that, delegates to the national protection authorities, under the supervision and coordination of the EDPS, the task of establishing and publishing a positive and negative list of processing operations subject or not to the obligation.[20] It should be added that the lists adopted by the GDPR and by the supervisory authorities are not exhaustive. As G. 29

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 and seq.

17. This paragraph refers to our book: *Le RGPD au défi de l'intelligence artificielle*, Cahier No. 48 du CRIDS, Brussels, Larcier, 2021; see also among a large literature: M. MENECEUR, *L'intelligence artificielle en procès*, Brussels, Bruylant, 2020.

18. G.29, 4 October 2017, Guidelines on data protection impact analysis and how to determine whether processing "is likely to 'give rise to a high risk'" for purposes of Regulation 2016/679, WP. 248, Rev. 01 confirmed by the EDPS, successor to the Article 29 Working Party. The reader may also usefully refer to the commentaries of the GDPR, such as the one published by T. DOUVILLE, *Droit des données à caractère personnel*, Gualino, Lextenso, 2021, pp. 227 et seq.

19. Emphasis added by Recital 91. See also the G.29 guidelines (p. 12) which states that in this case the risk is increased because these new technologies of data collection (Internet of Things) and use may have unknown personal or social consequences.

20. Thus, the CNIL has established two lists (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). On these two lists, read the commentary by A. DEBET and N. METALLINOS in *Comm. Comm Électr.*, January 2019. These guidelines were the subject, on 25 September 2018, of EDPS Opinion 9/2018.

notes,[21] "other operations may obviously present an equally high risk." This absence of a clear scope of the concept might create uncertainties for the data controllers.

Article 35(7) describes the minimum content of the analysis.[22] There is little description of the analysis procedure.[23] It must involve the data protection officer and, where appropriate, require the opinion of the data subjects or their representatives. In the event that the impact analysis reveals a high risk "if the controller does not take measures to mitigate the risk," Article 36(1)[24] requires the controller to consult the supervisory authority beforehand, which, if necessary, will react with a reasoned opinion, either by denouncing the legal violation or by considering that the risk has been incorrectly identified or insufficiently covered. It should be noted that it is up to the controller to decide whether or not to consult the supervisory authority, and it is therefore to be feared that he will interpret the conditions for recourse to the latter's opinion restrictively. Finally, the controller is required (Art. 35.11) to check whether the processing is carried out in accordance with the results of the analysis "at least when there is a change in the risk presented by the processing operations."

3. Beyond the Privacy Impact Assessment, the proposed regulation on artificial intelligence. On April 21, 2021, the Commission published its proposal for a regulation on AI: the "AI Act"[25] for short. Without doubt,

21. G.29, Guidelines already cited p. 10. G. 29 lists no less than 9 criteria that should be taken into account in this risk assessment and considers that the presence of two of these criteria should lead to the conclusion of the presence of a high risk. On this point, the comment of N. METALLINOS, "Consécration du rôle central des études d'impact sur la vie privée," 2017 *Comm. com. électr.*, comm. 57.

22. "The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned."

23. R. PERRAY, "Les outils de la conformité au RGPD: des outils de valorisation," 2021 RAE, Dossier special, C. CASTETS-RENARD, p. 44.

24. "The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk." At our opinion, that provision is too vague since it gives to the data controller a margin of appreciation about the criteria used by the provision and make them accountable in case of not having consulted the DPA, while it is considered by the latter that serious risks were existing.

25. This proposal is based on various documents: in particular, the White paper ("White paper on Artificial Intelligence – A European approach to excellence and trust," COM(2020) 65 final, 8), of February 2020 expresses the European "third way" strategy of an AI of excellence

this proposal does not deal with a theme as is the case with the GDPR, namely the protection of personal data, but rather to regulate the marketing of products or services because of the risks incurred by individuals, social groups or even society? We add that these products and services will very often use personal data, which implies the reference to the GDPR. Moreover, the risk-based approach, central to the justification of PIAs, is omnipresent in the proposal and the need to oblige those who design, market or use such products or services to assess and, if possible, reduce these risks responds to the same justification of "accountability."

The AI Act is based on a variable geometry of regulation according to the degree of risk presented by the technological applications. Thus, the text prohibits what it considers to be illegal AI practices[26] (Art. 5); it imposes specific transparency obligations on certain hidden applications, in particular AI's recognition of emotions; it subjects so-called "high-risk" applications to a system of evaluation, control and management (art. 6.2); and, finally, it leaves other applications presenting minimal risk to the self-regulation of the market. We will only mention[27] here the specific provisions relating to high-risk systems insofar as the proposed evaluation regime allows for a useful comparison with that put in place by the GDPR. This category is broad: on the one hand (Art. 6.1.), it concerns AI systems intended to be used in their own right or as safety components of products and subject by an existing regulation or directive to an *ex-ante* conformity assessment (for example, medical devices, financial and insurance products' delivery, devices embedded in games or motor vehicles, etc.).[28] On the other hand (Art. 6.2.), AI systems that mainly

and trust and the work of the HLGE on AI (High Level Group of experts on AI), including its publication of Ethical Guidelines for a Trustful RN (published on 8 April 2019), Ethics guidelines for trustworthy AI – Publications Office of the EU (europa.eu), available at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>. The seven criteria identified by the guidelines are respectively: Human Agency and Oversight; Technical Robustness and Safety; Privacy and Data Governance; Transparency; Diversity, Non-discrimination and Fairness; Societal and Environmental Well-being; Accountability. On the evaluation methods and criteria to be taken into account, see the Altai (Assessment List for Trustworthy AI), available at https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence.

26. Thus, manipulation systems by subliminal messages, the exploitation of vulnerabilities, the use by the public sector of "social ranking" systems leading to potential discrimination between people or groups, biometric systems operating in real time and remotely, placed in public places (e.g. facial recognition systems…).

27. For a more complete presentation, read Y. POULLET, "Vers un droit européen de l'intelligence artificielle," January 2022 *JDE* 284, pp. 454 et seq. and the references cited therein.

28. The many regulatory texts, which could be the source of such a safety obligation and therefore subject to the requirements of the AI Act if they use an AI system), are listed in Annex I. Thus, a medical robot, devices in so-called smart cars, credit rating systems used by financial organizations will now be subject to the requirements of the Medical Devices Regulation 2017 or the Motor Vehicles Regulation 2018 but in addition to the assessment obligation under the AI Act.

affect fundamental rights and are explicitly listed[29] in Annex III (biometric identification, access and evaluation in the education sector, evaluation of candidates in a recruitment procedure, police, justice, ...) as opposed to the GDPR approach which does contain a non-exhaustive list (*supra*, No. 2). We note that a large majority of these high-risk systems involve the processing of personal data, which is therefore also subject to the GDPR.

Providers of high-risk AI systems are subject to multiple duties (Art. 16). Such AI systems must meet certain requirements and be subject to an internal[30] *ex-ante* compliance assessment. The proposal requires the establishment, implementation, documentation and maintenance of a risk management system (Art. 9). It obliges to follow good practice in the evaluation of systems, in particular, the use of data sets that meet various quality criteria (representative, unbiased, geographically or behaviorally appropriate, etc.). Article 10 mentions various duties related to data governance, such as *testing* and validation of design choices and data taken into account, examination of possible biases and, given their purpose, obtaining an appropriate level of accuracy, robustness, cybersecurity, and consistency The requirement for technical documentation before the system is put on the market or put into service and its maintenance, documentation that is moreover detailed in its content and format by Annex IV of the proposal (Art. 11 and 18), while regretting that the transparency of the system's operation thus ensured concerns only the professional user of the system and not the end user, citizen or company, who will ultimately be sent the results of this operation. The ability to automatically record events ("logs") during the operation of AI systems (Art. 12 and 20) must be ensured. The assurance of a sufficiently transparent operation must allow users to interpret the results of the system and to use them appropriately. Finally, effective

29. Annex III contains a list of eight types of high-risk systems that may evolve: biometric identification systems (facial recognition, use of fingerprints, *etc.*), critical infrastructure management systems (road traffic, gas and electricity infrastructures, *etc.*), and security systems (e.g. firewalls, firewalls, *etc.*); critical infrastructure management systems (road traffic, gas and electricity transport infrastructures, *etc.*); applications in the education sector (e.g., education, health care, *etc.*); and applications in the education sector (e.g., education, health care, *etc.*); applications in the education and training sector (students' access and evaluation systems); employment applications (recruitment, control and evaluation of personnel); applications concerning access to or use of public services (in particular assistance systems) or private services (evaluation of the value of credit); systems used by law enforcement agencies (evaluation of the dangerousness of persons; reliability of means of proof, detection of emotions); systems used for migration or border control; systems for the administration of justice (research and interpretation of facts or interpretation and application of the law). The list can be modified by the Commission (Art. 7).

30. With some exceptions, it is the so-called "notifying" authority that will verify compliance (Art. 43). We note that in the area of AI systems for advertising recommendations or content used by the very large information and communication platforms, the proposed Digital Service Act (DSA for short) imposes this external audit, its publication and the duty of the platforms to comply with the recommendations of this audit.

supervision by natural persons during the period of use of the AI system (*human oversight*)[31] is required. The draft mentions the duty to cooperate with the competent national authorities, including by providing access to the systems and their documentation.

4. The assessment procedure under the IA Act[32]. Article 19 states: "providers of high-risk AI systems shall ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. Where the compliance of the AI systems with the requirements set out in Chapter 2 of this Title has been demonstrated following that conformity assessment, the providers shall draw up an EU declaration of conformity in accordance with Article 48 and affix the CE marking of conformity in accordance with Article 49." In particular, a quality management system "ensuring compliance with the regulation" must be put in place by suppliers of high-risk systems (Art. 17). For the vast majority of high-risk AI systems, suppliers (Art. 43), suppliers or users follow an internal[33] conformity assessment procedure referred to in Annex VI, which does not provide for the intervention of a notified body.[34] They will have to demonstrate that they have followed the harmonized standards, where they exist.[35] The regulation provides that certain high-risk

31. Art. 14.1: "High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use." Note the vagueness of such a provision.

32. For comparison, read the Privacy Impact Assessment Guide, published by the US Office of Personnel Management in April 2010, and the appendices issued by jurisdictions required to complete the PIA, if necessary. Jurisdictional reports about the PIA cases are also published.

33. With some exceptions listed in Annex VII. In this regard, the criticisms addressed by a collective of authors who stress the need to extend external auditing by accredited bodies to other high-risk AI systems: "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)." See N. SMUHA, E. AHMED-RENGERS, A. HARKENS *et al.*, "How the EU can achieve legally trustworthy ai: a response to the european commission's proposal for an artificial intelligence act?," 5 August 2021, *Leads Lab @ University of Birmingham*, p. 3 and developed pp. 48 et seq., text available at https://ssrn.com/abstract=3899991.

34. "Each Member State shall designate or establish a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring" (notified bodies) (Art. 30). The conditions and the procedure for the designation of the notified bodies by the national authorities, known as notifying authorities, as well as their respective competences are described in Articles 30 and s.

35. Art. 40: "High-risk AI systems which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title, to the extent those standards cover those requirements." It should be added that, in the absence of harmonized standards, the Commission may itself, after consulting the experts concerned

systems must be checked for conformity by the notified bodies designated by the notifying authority and will be issued by the latter, "after information has been given, in accordance with Article 46.3, to the other notified bodies carrying out similar activities", with a certificate in accordance with the procedure in Annex VII.[36] A database of high-risk systems listed in Annex III will be created. Obligations for suppliers to update and notify serious incidents are added and managed by the Commission (Art. 60). It is worth noting that there is no obligation to appoint a "compliance officer," as is the case in the area of data protection with the creation of a Data Protection Officer, whose role in the area of PIA has been emphasized. Of course, on this point, there are some exceptions.[37] Finally, the market surveillance authorities ensure compliance with the regulatory requirements and have broad access to the data, documentation and even the source code of the AI system (Art. 63 et seq.). They may, even for a compliant system that would nevertheless present a risk to health, safety or fundamental rights, invite "the relevant operator to take all appropriate measures to ensure that the AI system concerned, when placed on the market or put into service, no longer presents that risk, to withdraw the AI system from the market or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe." Finally, sanctions are possible[38] in the form of administrative fines (Art. 71 et seq.).

5. A comparison of the two regimes – the risks taken into account. Both texts clearly base the assessment obligation on a "risk-based approach."[39] Article 35 of the RGPD specifies the nature of the

and in accordance with a procedure laid down in the regulation (Art. 74 et seq.), draw up the list of "common specifications" necessary to meet the requirements of the regulation (Art. 41).

36. Annex VII provides for the control of both the quality management system and the documentation. Concerning the documentation system, Article 4.6 of annex VII provides: "Where the AI system is in conformity with the requirements set out in Title III, Chapter 2, an EU technical documentation assessment certificate shall be issued by the notified body. The certificate shall indicate the name and address of the provider, the conclusions of the examination, the conditions (if any) for its validity and the data necessary for the identification of the AI system. The certificate and its annexes shall contain all relevant information to allow the conformity of the AI system to be evaluated, and to allow for control of the AI system while in use, where applicable."

37. We note (Art. 15 of regulation on medical devices, L.117/165, 5 May 2017) that "Manufacturers shall have available within their organisation at least one person responsible for regulatory compliance who possesses the requisite expertise in the field of medical devices."

38. To note: "Before taking decisions pursuant to this Article, the European Data Protection Supervisor shall give the Union institution, agency or body which is the subject of the proceedings conducted by the European Data Protection Supervisor the opportunity of being heard on the matter regarding the possible infringement. The European Data Protection Supervisor shall base his or her decisions only on elements and circumstances on which the parties concerned have been able to comment. Complainants, if any, shall be associated closely with the proceedings." It should be noted that only administrative sanctions are explicitly stated, and nothing is said about other measures, such as withdrawal of the product from the market, compliance orders, *etc*."

39. See Art. 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks," 30 May 2014, WP 218.

risks that trigger the PIA obligation. The notion of "high risk" refers to data processing operations that are or may be likely to have a significant adverse impact on the fundamental rights and freedoms of natural persons. The term "likely to" does not mean that there is a remote possibility of a significant impact. The significant impact must be more likely than not. On the other hand, it also means that it is not necessary that people are actually affected: the likelihood that they will be significantly affected is sufficient.

These are "risks to the rights and freedoms of data subjects," in other words, those that the GDPR intends to protect according to Article 1.2. For Douville, but his broad interpretation is questionable, the expression could cover, "beyond the right to privacy and protection of personal data, freedom of movement, equality and absence of discrimination, the right to health, freedom of enterprise or the right to respect for property".[40] In support of this broad interpretation, we find the willingness of the Parliament's LIBE Committee to make an amendment during the discussion on the adoption of the GDPR that specifically includes the risks of discrimination in the scope of risks created by processing. Birnns[41] notes that this amendment was subsequently rejected but adds that Recital 75 still mentions this risk. In short, it is unclear at this time whether, under Article 35 of the GDPR, equality and discrimination issues should be considered when assessing the potentiality of risk from data processing. This question is important if we consider, for example, the use of biometric or genetic data, which are subject to risks of individual freedom as well as collective discrimination and which are to be viewed in the context of processing by AI systems, as high-risk systems.

Precisely, the proposal concerning AI systems clearly broadens the debate. It intends to consider not only the risks incurred by our individual liberties or jeopardizing our interests as consumers (see the systems of recommendation of goods or products) but also the risks of discrimination and non-respect of the values of social justice or even the societal risks, such as environmental issues, the attacks on the rule of law and

40. T. DOUVILLE, *Droit des données à caractère personnel*, *op. cit.*, 479, p. 228. It is noted that the so-called Article 29 Panel, in its guidelines on the DPIA of 4 April 2017 already cited, also refers, but incidentally, to the risks of 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*."

41. R. BIRNNS, "Data Protection impact assessment: a meta regulatory approach," 2017 *Int. data &Privacy Law* 7, p. 28.

democracy.[42] Thus, when referring to the "fundamental rights" challenged by AI and which the proposal aims to protect, point 3.5 of the explanatory memorandum stresses: "the use of AI with its specific characteristics (e.g. opacity, complexity, dependency on data, autonomous behaviour) can adversely affect a number of fundamental rights enshrined in the EU Charter of Fundamental Rights ('the Charter'). This proposal seeks to ensure a high level of protection for those fundamental rights and aims to address various sources of risks through a clearly defined risk-based approach. With a set of requirements for trustworthy AI and proportionate obligations on all value chain participants, the proposal will enhance and promote the protection of the rights protected by the Charter: the right to human dignity (Art. 1), respect for private life and protection of personal data (Art. 7 and 8), non-discrimination (Art. 21) and equality between women and men (Art. 23). It aims to prevent a chilling effect on the rights to freedom of expression (Art. 11) and freedom of assembly (Art. 12), to ensure protection of the right to an effective remedy and to a fair trial, the rights of defence and the presumption of innocence (Art. 47 and 48), as well as the general principle of good administration. Furthermore, as applicable in certain domains, the proposal will positively affect the rights of a number of special groups, such as the workers' rights to fair and just working conditions (Art. 31), a high level of consumer protection (Art. 28), the rights of the child (Art. 24) and the integration of persons with disabilities (Art. 26). The right to a high level of environmental protection and the improvement of the quality of the environment (Art. 37) is also relevant, including in relation to the health and safety of people. The obligations for ex ante testing, risk management and human oversight will also facilitate the respect of other fundamental rights by minimizing the risk of erroneous or biased AI-assisted decisions in critical areas such as education and training, employment, important services, law enforcement and the judiciary." In other words, the proposed AI regulation intends to broaden the scope of evaluation from that to which the GDPR was limited. According to the text of the proposal, "it complements these acts (the GDPR but also other acts such as the one on non-discrimination, gender equality, security, consumer protection, etc.) with a set of harmonized rules on the design, development and use of certain high-risk AI systems as well as restrictions on certain uses of remote biometric identification systems..."

42. On the consideration of these three categories of risks, present in international texts on AI ethics, read Y. POULLET, "About some international documents relating to the ethics of Artificial Intelligence – Some insights," in *Time to reshape Information Society*, Proceedings of the 40th anniversary of the CRIDS (under the direction of H. Jacquemin), notebook of the *CRIDS* No. 52, pp. 501 et seq.

The ethical values assessment proposed therefore goes beyond that imposed by the PIA and is appropriate when it comes to processing personal data using AI systems. Three comments on this subject: the first is the magnitude of the work[43] and skills to be gathered or coordinated when it will be necessary to proceed on the occasion, for example, of the evaluation of applications intended for the piloting of intelligent cars, to confront concerns of data protection, consumers, environment and non-discrimination ; the second is the role of the PIA, within this overall evaluation, to be conducted separately and then transmitted to the report desired by the regulatory proposal; third, we know that the EDPS[44] has called for data protection authorities to be the future notification authorities, justifying their competence and experience in PIA. The enlargement we have discussed, however, undermines this claim. It is certain that other independent administrative authorities or bodies, such as the Public Centers for equal opportunities, the authorities in charge of freedom of expression within the audiovisual sector, the consumer protection or competition Commisions, etc., must also play a role in view of such an enlargement, with the obvious risk of tensions and even contradictions between these opinions.[45] This being said, it is legitimate to recognize, in view of the major and often prevalent risks of data protection infringement, incurred due to the use of AI systems and their particularity of prediction, profiling and opacity of functioning, a certain priority to this protection and the presence of a member of the EDPS in the European Committee on Artificial Intelligence[46] which oversees or rather coordinates all the national control and monitoring bodies, having a role in regulating the various AI risks.

In any case, the need for a transversal approach, as proposed by the Commission in relation to AI systems, can, in our opinion, only be achieved by clarifying the role and competences of each category of administrative

43. In this respect, one remains doubtful about the possibility of considering all the risks in view of the number of provisions contained in the European charter of fundamental rights.

44. EDPB/EDPS, *Joint opinion /2021 on the proposal for a regulation laying down harmonized rules on Artificial intelligence*, 18 June 2021, in particularly the footnote 52.

45. Let us take the hypothesis of an AI system allowing the calculation of life or vehicle insurance premiums as close as possible to the risks associated with each insured. This system could, in particular, with the guarantee of individual informed consent, be judged as compliant with the requirements of the RGPD and, on the other hand, judged as discriminatory by an organization in charge of fighting against discrimination, on the grounds that the reduction in premiums obtained by those deemed to be good performers leads to a disproportionate additional cost for others and proves to be contrary to the principle of pooling of these risks.

46. "The Board shall be composed of the national supervisory authorities, who shall be represented by the head or equivalent high-level official of that authority, and the European Data Protection Supervisor. Other national authorities may be invited to the meetings, where the issues discussed are of relevance for them." (Art. 57).

authorities but, above all, by the institutionalized creation of places for dialogue between these different bodies, without which there is a risk of interventions in contradictory directions or even rivalry between authorities.

6. A common preventive approach. The risk-based approach has another consequence: it fully justifies the shift from a classical legal drafting – based on the definition of behavioral contents to be respected and, in case of non-compliance, on the repression or the a posteriori sanctioning of infringements of the regulation – to an a priori approach based on the obligation of risk assessment, i.e. the setting up of a risk assessment procedure and the monitoring of compliance with this procedure. The preventive risk-based approach seems to be a common feature of the two regulatory texts studied. The "Privacy Impact Assessment" introduced by the RGPD, thus shifts the scope of the regulation towards a preventive approach to avoid or reduce risks by the need to set up an assessment procedure at the design stage of the processing. The same idea runs through the AI Act proposal, which develops this procedure at leisure, defining its stages, its content, the quality and risk management implemented, etc. This approach is certainly more cumbersome administratively and can therefore only be justified under the proportionality principle in cases of significant risk.

The procedural differences in the evaluation are certainly remarkable. Articles 35 and 36 of the GDPR describe at least the steps and the actors to be involved in this assessment. The criteria for risk assessment are described in a vague manner, even though the Group 29 guidelines have clarified them somewhat.[47] In this respect, the IA Act is much more complete. The documentation to be provided (Annex VI), the information necessary for the registration of AI systems with the data bank in order to establish their compliance (Annex VIII) are carefully detailed, and above all the supplier must develop a quality management system, the characteristics of which are carefully specified in Article 17.[48] Finally, the criteria for assessing 'high risk' listed in Article 6.2 are specified.[49]

47. See G.29, Guidelines, on Data Protection Impact Assessment (DPIA), issued 4 October 2017, WP 248, pp. 11-12. The group establishes 9 criteria. See also, on this basis, the lists drawn up by the national authorities.

48. Art. 17: "Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects […]."

49. "When assessing for the purposes of paragraph 1 whether an AI system poses a risk of harm to the health and safety or a risk of adverse impact on fundamental rights that is equivalent to or greater than the risk of harm posed by the high-risk AI systems already referred to in Annex III, the Commission shall take into account the following criteria:

(a)the intended purpose of the AI system;

(b)the extent to which an AI system has been used or is likely to be used;

Another common preventive instrument is the affixing of a certificate of compliance. The GDPR, on the one hand, and the proposed regulation, on the other, mention certificates as methods of verifying compliance with regulatory requirements, but their respective roles are different. Under Article 42 of the GDPR, certification is voluntary, based on its granting by certification bodies, under procedures and on the basis of criteria defined by the supervisory authority. Under the proposal, certification of compliance by the notification authorities is mandatory for high-risk systems and covers elements based on harmonized European standards (see Regulation No. 1025/2012)[50] and specifications established by the Commission. It is therefore clear that the certification obtained under the proposal does not correspond to the specific one on data protection and has other objectives.[51] It is therefore understandable that the EDPS and the EDPS in their attached opinion (No. 23) demand that the certificate of conformity of high-risk AI systems also covers compliance with the requirements of the GDPR: "To

(c)the extent to which the use of an AI system has already caused harm to the health and safety or adverse impact on the fundamental rights or has given rise to significant concerns in relation to the materialisation of such harm or adverse impact, as demonstrated by reports or documented allegations submitted to national competent authorities;

(d)the potential extent of such harm or such adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons;

(e)the extent to which potentially harmed or adversely impacted persons are dependent on the outcome produced with an AI system, in particular because for practical or legal reasons it is not reasonably possible to opt-out from that outcome;

(f)the extent to which potentially harmed or adversely impacted persons are in a vulnerable position in relation to the user of an AI system, in particular due to an imbalance of power, knowledge, economic or social circumstances, or age;

(g)the extent to which the outcome produced with an AI system is easily reversible, whereby outcomes having an impact on the health or safety of persons shall not be considered as easily reversible;

(h)the extent to which existing Union legislation provides for:

(i)effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages;

(ii)effective measures to prevent or substantially minimise those risks."

50. Regulation (EU) No. 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No. 1673/2006/EC of the European Parliament and of the Council…

51. "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 Art. 42(2) with regard to certifications issued under Regulation (EU) 2019/881) (That regulation is specific to cybersecurity). 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 (already mentioned)*, No. 74.

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. Different actors? As far as the actors are concerned, we note that the evaluation obligation concerns, according to the terminology of the GDPR, the controller and, exceptionally, the processor; the proposal, following its logic of considering the AI system as a product (or service) that is placed on the market, addresses this obligation to the "provider" of the AI "product," This approach contrasts with the GDPR one, which focuses on the use of this product or services and will often be considered as the "user" of the AI system in the context of the application of the AI Act. The notion of "provider" is defined by Article 3 (2) as follows*:* "'provider'[52] means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge." It should be noted that the provider is therefore often a person other than the controller of the data processing: thus, when a company develops a consumer profiling system, which it implements at various retailers, or a surgical robot that it sells to hospitals, it can only be a controller of the personal data that it would use in the context of the product development tests. On the other hand, if it is a "provider" in the sense of the proposal, its client, which will operate the system and will undoubtedly process much more data than the company that developed the algorithm, will, according to the proposed regulation, be qualified under the AI Act as a user[53] and will bear much less responsibility on the basis of the latter, while being responsible in the sense of the GDPR and therefore bound, under the conditions of the latter, to a PIA. Then, we note that while the GDPR limits the duties related to the processing to the only persons in charge and subcontractors, the AI Act considers all the actors[54] of the chain that goes from the conception of the product to the end of its use and prescribes reciprocal obligations of some actors towards others, in particular in terms of documentation and collaboration between them, as well as the data furnisher towards the provider of the AI system, the

52. In the latest version of the AI Act, the term of "operator" has been retained instead of "provider" but the definition remains the same.

53. Art. 3(4): "'user' means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity."

54. This same concern can be found in the recent recommendation of the Council of Europe.

provider towards the user[55] and vice versa.[56] This tendency to create obligations between the members of the chain of actors whose collaboration is necessary for the realization of a treatment is also found in the field of data protection, in particular in the text of the recent recommendation of the Council of Europe on profiling.[57]

8. From co-regulation to the societal responsibility of certain actors. Some authors[58] see the possibility for companies or administrations, at the end of an internal evaluation procedure, to determine for themselves the manner in which they intend to respond to the risks generated by the treatments they envisage as a form of co-regulation or, to be more precise, as the result of a "meta-regulatory" approach, defining this as "any form of regulation (whether by tools of state law or other mechanisms) that regulates another form of regulation," in this case "the legal meta-regulation of internal corporate selfregulation."[59] This analysis, which we have defended on several occasions,[60] is interesting insofar as it refers to the social responsibility of the company or the administration to assume, within a defined regulatory framework, through the evaluation procedure, the risks that its information system project poses, within the framework of Article 35 of

55. For instance, Art. 21: "Providers of high-risk AI systems which consider or have reason to consider that a high-risk AI system which they have placed on the market or put into service is not in conformity with this Regulation shall immediately take the necessary corrective actions to bring that system into conformity, to withdraw it or to recall it, as appropriate. They shall inform the distributors of the high-risk AI system in question and, where applicable, the authorised representative and importers accordingly."

56. Art. 29(2) and (4).

57. Recommendation CM/Rec(2021)8 of the Committee of Ministers to Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted by the Committee of Ministers on 3 November 2021. Thus, Art. 3.12: "When acquiring data or algorithms from a third party, the controller(s)or processor(s) should obtain from the third party the documentation necessary to check the quality of the data and algorithms and their relevance to the purpose of the processing." On the arguments imposing this duty to create obligations vis-à-vis actors other than only data controllers and processors, in the texts on data protection, read B. FRENAY and Y. POULLET, "Profiling and Convention 108+: Report on developments after the adoption of Recommendation (2010)13 on profiling," October 2020, *Comité consultatif de la Convention* 108+, Strasbourg, T-PD(2019)07FINAL, available at https://rm.coe.int/t-pd-2019-7final-en-2757-5764-0706-1-2776-1394-9442-1/1680a0925c.

58. See in particular, D. WRIGHT, "Making Privacy Impact Assessment More Effective," 2013 *The Information Society* 29:5, pp. 307-315, DOI: 10.1080/01972243.2013.825687; R. BINNS, "Data Protection impact assessment", International Data Privacy assessments: a meta-regulatory approach," 2017 *International Data Privacy Law* 7:1, pp. 29-30.

59. The definition is taken from C.E. PARKER, *The Open Corporation Effective Self-Regulation and Democracy*, Cambridge University Press, 2002. The author believes that self-regulation can only be taken seriously and be effective if it is based on a legal requirement and framework.

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

the GDPR, to the persons concerned and, within the framework of the AI Act, beyond individual liberties, to certain communities, social justice, the environment, public health and democracy.[61]

The response of the entity concerned may be original and innovative; what is important is that the procedure has been properly conducted. The attention is put as much on the procedure as on the result. This leads us to underline some deficient points in the two texts analyzed. The first point, in the name of the legitimacy of the document to be produced, would indeed require the participation of all the representatives of interests linked to the envisaged functioning of the system. We know that the first versions of the GDPR would require the opinion of the data subjects during the evaluation; Article 35.6 now only envisages this opinion "where appropriate" and "without prejudice to the protection of general or commercial or public interests or the security of processing operations." The same shortcoming is deplored in the proposed AI Act. Another criticism is the absence of any obligation to publish a report on the assessment produced. This obligation, affirmed in the first versions of the GDPR, was abandoned in the final version, even though the opinion of the Group 29 recommends it, while stressing that many objections related to business secrecy and intellectual property may oppose it. In the framework of the AI Act, Annex 5 relating to the declaration of conformity does not mention the obligation to file an evaluation report, even if the mandatory documentation that accompanies the product provides a certain amount of information on the quality of the product, the evaluation it has undergone and the risks related to its operation, but only for the attention of professional users who will implement the applications enabled by the AI system provided. These two points seem important to us. Without the participation of all the stakeholders and a report made available to the public, the result of the evaluation and quality management procedures for the protection of individuals, groups and society risks being

61. "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 behavior 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." See N. SMUHA, E. AHMED-RENGERS, A. HARKENS *et al.*, "How the EU can achieve legally trustworthy ai: a response to the European commission's proposal for an artificial intelligence act?," 5 August 2021, *Leads Lab @ University of Birmingham*, p. 6, available at https://ssrn.com/abstract=3899991.

purely formal and leading to minimal compliance. Beyond mere compliance, processing and systems, is it not required to pursue the desired ethical and legal values? Finally, we note that in both texts, the supervisory authorities have the right to have access to this evaluation report and that its absence or non-compliance with the legal evaluation procedure imposed may be sanctioned by an administrative penalty.

9. From specific Impact Assessments to the creation of multidisciplinary coordination bodies for the "ethical" evaluation of high-risk or high-risk systems. Beyond the Privacy Impact Assessment and the Ethical Values Impact Assessment advocated by the two texts with regard to specific so-called high-risk treatments or so-called high-risk AI systems, should we not foresee a broader reflection when the issues related to an emerging technology require societal choices? Thus, to take just a few examples, facial recognition, recommendation systems used by gatekeepers or large platforms, genetic data processing, and one-to-one insurance cannot be decided at random by the various impact studies carried out on the occasion of the many projects in question but must be the subject of a general reflection and even, if necessary, of specific regulatory provisions. This need for public discussion and participation of civil society on the issues at stake seems to us to be carried out within an open European forum of "Data Ethics." As N. SMUHA et alii[62], in a particularly critical commentary on the AI Act proposal, the proposal presents an important gap, that of the absence of consideration of the right to citizen participation in the societal choices that technological advances are shaping: "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 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."

62. N. SMUHA *et al.*, report already cited, p. 3 and expanded on pp. 48 et seq., available at https://ssrn.com/abstract=3899991.

Beyond the internal evaluation procedure of companies or administrations established for specific applications, it would be useful, in order to support this internal procedure, for the European Union, if at least it follows the orientations of the White Paper of January 2020 issued by the Commission, to move, on the basis of the models adopted by countries[63] such as Denmark, Germany[64] or the United Kingdom,[65] towards *the creation of a multidisciplinary body for the 'ethical' evaluation of AI systems*.[66] The role of this "independent multidisciplinary authority for the evaluation of risks linked to artificial intelligence" would be to coordinate the activities of the national authorities created each in their specific field of competence (environment,

63. "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).

64. The German Federal Data Ethics Kommission was established on 5 September 2018. Its membership includes industry representatives, ODA representatives, and others. It recently (October 2019) published a major report on the development of artificial intelligence systems, available at https://datenethikkommission.de/wp-content/uploads/191015_DEK_Gutachten_screen.pdf. She suggests regulation of AI systems based on the potential for harm to the individual and society: "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.

Systems with unwarranted potential harm such as autonomous weapons should be 'fully or partially' forbidden." (Summary proposed by Algorithmwatch)

65. About the UK's Data Ethics and Innovation Authority, see the authority's website: https://www.statisticsauthority.gov.uk/about-the-authority/committees/nsdec/data-ethics/: "The UK Statistics Authority aims to mobilize 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 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."

66. The Council of Europe is also moving towards such a recommendation to the Member States. In this respect, the Report on Artificial Intelligence submitted by A. Mantelero to the Council of Europe (this report served as a basis for the establishment of the Guidelines adopted by the Council of Europe in the field of artificial intelligence), in particular pages 16 et seq. The author underlines the interest of an approach at a national level as a complement to the implementation of a procedure at the level of companies. Cf. also the Frenay-Poulet report already cited on profiling of November 2019 to the Advisory Committee on Convention No. 108, report already cited, p. 42 and following.

security, social justice, consumer protection, data protection), in order to coordinate the competences, rules and criteria for the evaluation of AI systems.[67] In this perspective, we should undoubtedly review the composition[68] and functioning of the European Artificial Intelligence Committee established by the AI Act and, among its competences, develop the one mentioned in Article 56.2 (b), i.e. "coordinate the guidelines and analyses of the Commission and of the national supervisory authorities and other competent authorities on emerging issues throughout the internal market in matters covered by this Regulation, and contribute to these guidelines and analyses […]."

CONCLUSION

10. Is risk assessment an excellent initiative? This paper highlights the value of the approach. It is rightly based on a risk-based approach, which allows for asymmetrical and more proportionate regulation according to the treatments and technologies used; it presupposes the accountability of the actors and obliges them to carry out an *a priori* evaluation and corrective measures[69]. That said, both proposals have shortcomings:

– They are based on internal risk self-assessment.[70] It is undoubtedly difficult, if only to avoid handicapping European innovation by cumbersome and inappropriate external audit procedures, to impose

67. "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).

68. This authority must be open to different categories of people interested in AI applications (representatives of workers, consumers, civil liberties associations, *etc.*). "A European governance structure on AI in the form of a framework for cooperation of national competent authorities (i.e. not only data protection authorities but also consumer protection authorities, competition authorities, audiovisual authorities, equal opportunities authorities,...) 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).

69. "[The proposal represents] 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" (Explanatory memorandum to the AI Act proposal, cited above, p. 3).

70. "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

external control[71]. However, this choice would have required counterbalances to the decisions of the data controllers, the participation of representatives of the people who are likely to be subject to the risks linked to the technology, the publication of the report[72] and the presence, as required by the GDPR, of a «compliant officer.» It is also to be feared that those responsible or suppliers who wish to avoid the application of the mandatory provisions for high-risk processing or high-risk AI systems will plead the non-existence of such risks in the concrete cases they are dealing with or that the reports will be reduced to the result of a purely formal obligation.

– The interaction between the two types of evaluation is not obvious: the first is based on compliance with a regulation whose content and principles are particularly well developed, but which leaves in the dark many details of the procedure to be put in place; the second appears to be centered on a product or service placed on the market, carefully detailing the procedure and the tools for managing it, and referring to numerous values to be complied with, but without specifying the principles imposed by compliance with its values. Without a doubt, and a reading of the so-called high-risk AI systems, as listed in Annex 3 of the proposed AI Act Regulation, attests to this, the

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 thatthe 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.*, report already quoted, pp. 48 et seq.)

71. As would be imposed on 'very large information and communication platforms' (i.e. social networks and search engines with a customer base equal to or greater than 10% of the European population) if the proposal known as the Digital Service Act of the European Commission under discussion. According to this proposal, these platforms would be required to conduct assessments of so-called systemic risks caused by or related to the operation and use of their services (Art. 26) and to take reasonable and effective measures to mitigate these risks (Art. 27). They must also submit to external and independent audits (Art. 28). In cases where very large online platforms use referral systems (Art. 29) or display online advertising on their online interface (Art. 30), they are also subject to specific transparency obligations. They will grant access to data to researchers to understand how online risk is evolving; they appoint one or more compliance officers to ensure compliance with the obligations set out in the regulation (Art. 32); and they have specific and additional transparency reporting obligations (Art. 33).

72. We note that Art. 27 of the Data Protection and Police Directive provides for the publication of the evaluation report. "1. Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data. 2. The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned."

risks related to data protection of future AI applications are a major element of the Commission's concerns and have significantly justified the regulatory proposal. It is clear that AI systems increase by their opacity, by their processing capabilities out of all proportion to the traditional ones, including those to predict our lives, by the risks of bias and errors undoubtedly justifies the crucial role of DPAs and compliance with the GDPR. However, should we reduce the evaluation of AI systems to the consideration of these risks alone? We do not think so, and it is undoubtedly one of the merits of the AI Act to have highlighted the need to take into consideration other risks, this time collective or societal, and to advocate for closer collaboration between the various bodies in charge of these broader concerns than those purely individual.