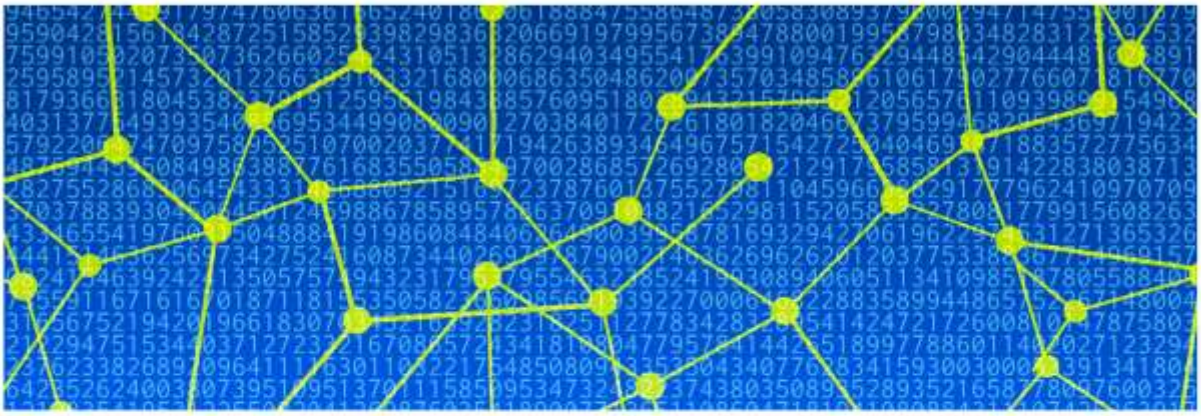

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 4/2020

EDPS Opinion on the European Commission’s White Paper on Artificial Intelligence – A European approach to excellence and trust

29 June 2020

Executive Summary

On 19 February 2020, the European Commission published a White Paper on "Artificial Intelligence: A European approach to excellence and trust". It is part of a wider package of strategic documents, including also a Communication on "A European strategy for data".

The aim of the White Paper is twofold: setting out policy options to promote the uptake of Artificial Intelligence ('AI') and to address 'the risks associated with certain uses of this new technology'. To achieve such goals, the White Paper proposes a set of actions to foster the development and the adoption of AI and a new regulatory framework that would address concerns specific to AI that the current framework may not address.

This Opinion presents the EDPS views on the White Paper as a whole, as well as on certain specific aspects, such as the proposed risk-based approach, the enforcement of AI regulation or the specific requirements for the remote biometric identification (including facial recognition).

The EDPS acknowledges AI's growing importance and impact. However, AI comes with its own risks and is not a 'silver bullet' that will solve all problems. Benefits, costs and risks should be considered by anyone adopting a technology, especially by public administrations who process great amounts of personal data.

The EDPS very much welcomes the White Paper's numerous references to a **European approach to AI,** grounded in **EU values and fundamental rights** and the consideration given to the need for **compliance with the European data protection legislation**.

Hence, the aim of the recommendations in this Opinion is to clarify and, where necessary, further develop the safeguards and controls with respect to protection of personal data, taking into consideration the specific context of AI.

To this end, the EDPS recommends in particular that any new regulatory framework for AI:

- **applies both** to EU Member States and to EU institutions, offices, bodies and agencies;

- is designed to **protect from any negative impact**, not only on individuals, but also on communities and society as a whole;

- proposes **a more robust and nuanced risk classification scheme**, ensuring any significant potential harm posed by AI applications is matched by appropriate mitigating measures;

- includes an impact assessment **clearly defining the regulatory gaps** that it intends to fill.

- **avoids overlap** of different supervisory authorities and includes a cooperation mechanism.

Regarding remote biometric identification, the EDPS supports the idea of **a moratorium on the deployment, in the EU, of automated recognition in public spaces of human features**, not only of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, so that an informed and democratic debate can take place and until the moment when the EU and Member States have all the appropriate safeguards, including a comprehensive legal framework in place to guarantee the proportionality of the respective technologies and systems for the specific use case.

The EDPS remains at the disposal of the Commission, the Council and the European Parliament to provide further advice, and expects to be consulted in due course as foreseen in Article 42 of the Regulation (EU) 2018/1725. The comments in this Opinion are without prejudice to additional comments in the future on particular issues and/or if further information becomes available.

TABLE OF CONTENTS

1. INTRODUCTION AND BACKGROUND 5

2. GENERAL OBJECTIVES AND VISION 6

3. NECESSITY OF AN AMENDED LEGAL FRAMEWORK 8

4. ASSESSMENT OF THE FUTURE REGULATORY FRAMEWORK FOR AI 10

4.1. Precautionary principle and risk-based approach 10

4.2. Data Protection Impact Assessment 15

4.3. Accountability and enforcement 17

4.4. Regulatory requirements 18

4.5. Controls and governance 19

5. OTHER SPECIFIC ISSUES 20

5.1. Remote biometric identification 20

5.2. Vulnerable groups 21

5.3. Access to data 22

6. CONCLUSIONS 22

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, 'GDPR')[1],

Having regard to 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[2],

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC[3] ('EUDPR'), in particular Articles 57(1)(h) and Article 58(3)(c),

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

1. The Commission White Paper 'On Artificial Intelligence– A European approach to excellence and trust'[4] ('the White Paper') is part of the initiative No. 10 ('A European Approach to AI') and falls under the 'Chapter' 'A Europe Fit for the Digital Age' of the Commission Work Programme 2020.

2. The EDPS notes that the White Paper is closely linked to the 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - a European strategy for data'[5] ('the Data Strategy'), in relation to which the EDPS has adopted a separate Opinion[6].

3. The EDPS was consulted by the Commission on 29 January 2020 on the draft of the White Paper and submitted preliminary informal comments. The EDPS welcomes the fact that his views have been sought at an early stage of the procedure and encourages the Commission to continue with this good practice.

[1] OJ L 119, 4.5.2016, p. 1.

[2] OJ L 119, 4.5.2016, p. 89.

[3] OJ L 295, 21.11.2018, p. 39.

[4] COM (2020) 65 final.

[5] COM (2020) 66 final.

[6] EDPS Opinion 3/2020 on the European strategy for data, https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf

4. The White Paper is subject to public consultation. The objective of the consultation is to collect views on the White Paper as a whole, as well as on certain specific aspects. A similar public consultation had been launched on the European Commission's Communication 'A European strategy for data'.

5. This opinion elaborates upon some of the EDPS' informal comments and provides more targeted input to the European Commission in light of the public consultation. Furthermore, this opinion is without prejudice to any additional comments that the EDPS could make based on further available information at a later stage, including in the context of the future legislative consultations on the legal acts foreseen in the White Paper and Commission Work Programme.

6. Although European Union institutions, bodies, offices and agencies are subject to the EUDPR instead of to the GDPR, both regulations pursue the same objectives and their principles are identical.[7] To reflect this coherence, any reference to a GDPR provision in this opinion will also indicate the corresponding EUDPR provision in parentheses.

7. In the interest of a **coherent approach throughout the Union**, the EDPS recommends that any new regulatory framework for AI applies both to EU Member States and to EU institutions, offices, bodies and agencies. **Where Union institutions, bodies, offices and agencies make use of Artificial Intelligence ('AI'), they should be subject to the same rules as those applying in EU Member States.**

2. GENERAL OBJECTIVES AND VISION

8. The EDPS very much welcomes the White Paper's numerous references to a European approach to AI, grounded in **EU values and fundamental rights** and the consideration given to the need for compliance with the European data protection legislation. At the same time, the EDPS expects **this firm commitment to be fully reflected in any new European regulatory framework for AI** in order to achieve an effective respect of fundamental rights and values, including human dignity, pluralism, equality, non-discrimination, the rule of law, due process and the protection of private life and of personal data.

9. The EDPS recalls that, pursuant to Article 5 of the GDPR and Article 4 EUDPR, the processing of personal data should always respect the **general principles** of lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality as well as accountability of the controller.

10. The White Paper declares having a twofold objective, setting out policy options to promote the uptake of AI and to address 'the risks associated with certain uses of this new technology'. Given these objectives, the EDPS agrees with the Commission that the term AI needs to 'be clearly defined for the purposes of this White Paper as well as any possible future policy-making initiative'. The EDPS regrets however that the document presents more than one definition and does not clearly embrace any of them: the White Paper first defines

[7] Whenever the provisions of Regulation (EU 2018/1725) follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should, under the case law of the Court of Justice of the European Union be interpreted homogeneously, in particular because the scheme of the EDPR Regulation should be understood as equivalent to the scheme of the GDPR; see recital 5 EDPR, referring to ECJ judgment of 9 March 2010, *European Commission v Federal Republic of Germany*, Case C-518/07, ECLI:EU:C:2010:125 paragraph28.

AI as ’the combination of data, algorithms and computing power’; however the EDPS suggest that such definition is too ambiguous as it is applicable to other technologies too (e.g. ‘big data’). Later, the White Paper refers to the definitions included in the European Commissions’ Communication on AI for Europe’ and in the work of the High Level Expert Group on AI. The White Paper ends up leaving the task of defining AI for the ‘new legal instrument’. The EDPS is of the view that with **the White Paper the European Commission missed an opportunity to propose a clear definition for AI** that would serve to frame the scope of actions and possible future legislative proposals. In such situation, it will be difficult to understand what will be the scope of the possible legislation based on this White Paper. The EDPS is of the view that any AI definition for a future legal instrument should at least take into account the following elements: a decision-making model, an algorithm that translates this model into computable code, the data this code uses as an input and the environment surrounding its use.[8]

11. To achieve its objectives, the White Paper declares as one of its main building blocks to set out a policy framework ‘to create the right incentives to accelerate the adoption of solutions based on AI’. Moreover, the White Paper considers ‘*essential* that public administrations, hospitals, utility and transport services, financial supervisors, and other areas of public interest rapidly begin to deploy products and services that rely on AI in their activities.’[9] By labelling AI as an ‘essential’ technology, the White Paper seems to presume that it is the most appropriate technology regardless of the business processes of a public authority and the risks posed by its use. The EDPS is of the view that **there is no such thing as a technological ‘silver bullet’**. AI, like any other technology, is a mere tool, and should be designed to serve humankind.AI, like any other technology, has advantages and disadvantages and public authorities and private entities alike should consider on case-by-case basis whether an AI application is the best option to achieve important public interest outcomes.

12. In the same vein, the White Paper states that ‘A specific focus will be in the areas of healthcare and transport **where technology is mature for large-scale deployment**.’ (Emphasis added). The White Paper does not provide any reference to scientific evidence supporting such claim, and runs the risk of promoting a **blind uptake** of AI. The White Paper does not define the criteria used to assess AI’s maturity level in specific application areas.[10]The EDPS therefore suggests that a more profound and quantified analysis, based on identified sources, than currently present in the White Paper would strengthen the Commission's position and benefit the public debate about the White Paper by ensuring a heightened quality of the arguments.

13. The EDPS also believes that some AI applications (e.g. live facial recognition) interfere with fundamental rights and freedoms to such an extent that they may call into question the essence of these rights and freedoms. Due to the early stages of AI development or

[8]Inspiration for these elements can be found in the following documents: HLEG on AI ‘A definition of Artificial Intelligence: Main capabilities and disciplines‘, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341 and AlgorithmWatch, ‘Automating Society Taking Stock of Automated Decision-Making in the EU (2019)’, https://algorithmwatch.org/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf.

[9] White Paper on AI, section 4.F

[10] If one were to take the number of research studies conducted since 2013 on the use of AI in healthcare as a proxy for maturity, one will find quite different maturity levels (e.g. 531 studies on image processing and analysis, 45 studies on pathological analysis or 10 studies in disease management); see Journal of Biomedical Informatics, Volume 100, December 2019, ‘Transforming healthcare with big data analytics and artificial intelligence: A systematic mapping study’, https://www.sciencedirect.com/science/article/abs/pii/S1532046419302308

deployment and lack of full view of its impact on our society, the European Commission should advocate the strict application of the precautionary principle approach. This consideration will be further elaborated on the following sections.

3. NECESSITY OF AN AMENDED LEGAL FRAMEWORK

14. The EDPS welcomes the call for **full and effective application and enforcement of the existing EU legal rules,** as well as for careful and objective assessment of the need for any future legislative adjustments.

15. The EDPS also agrees with the approach put forward in the White Paper by which for AI systems operated in the EU '*it is paramount that EU rules are respected by all actors... regardless of whether they are based in the EU or not*', as this is consistent with the approach of the EU legislators chosen for the protection of personal data, in particular the GDPR.

16. **The European data protection legal framework is technology-neutral and is no obstacle for the successful adoption of new technologies, in particular AI**. On the contrary, it is meant to **foster the application of any technology** to the processing of personal data while in full respect of European values and fundamental rights.

17. The White Paper declares that its objective is to minimise the risks posed by AI and identifies the most significant ones as 'the application of rules designed to protect fundamental rights' and 'safety and liability-related issues**.**' The first type of risks are later detailed as affecting 'the rights to free expression, personal data protection, privacy and political freedoms'. In section 5.B, the White Paper specifies the risks and situations where the EU regulatory framework might need improvement to ensure proper enforcement:

    - The risk regarding the 'Effective application and enforcement of existing EU and national legislation' is articulated around the opaqueness of AI, which will be dealt with in the accountability and enforcement section below in section 4.3.

    - The risk 'Limitations of scope of existing EU legislation' is focused on the EU's product safety regulatory framework.

    - The 'Changing functionality of AI systems' risk, as described in the White Paper[11], is not new or exclusive to AI applications. The EDPS regrets that the White Paper does not explain in further detail why software upgrades adding new functionalities present compliance issues different from the ones posed by changing functionality to non-AI systems.

    - The 'Uncertainty as regards the allocation of responsibilities...' risk seems related to the EU legislation on product safety. Given that GDPR requirements must be met by data controllers and data processors in the context of AI applications when processing personal data, it is necessary to clearly assign these roles to adequately allocate responsibilities. A data protection impact assessment (DPIA) is a useful tool help allocate responsibilities.

[11] 'the integration of software**,** *including AI***,** into products can modify the functioning of such products and systems during their lifecycle' (emphasis added)

- The 'Changes to the concept of safety' relates to 'risks that EU legislation currently does not explicitly address' and is linked to the EU's product safety regulatory framework.

The links between these risks and specific legislative gaps triggering the need for the new regulation remain unclear. The impact assessment of any proposal for an AI regulatory framework should clearly include such links.

18. During the second half of 2019, over 350 organisations provided feedback[12] to the High-Level Expert Group Guidelines on trustworthy AI[13]. As part of that feedback, the White Paper mentions that the transparency[14], traceability[15] and human oversight,[16] key requirements in the High-Level Expert Group Guidelines[17], 'are not specifically covered under current legislation in many economic sectors'. The EDPS is of the view that the GDPR fully reflects the mentioned key requirements and it applies to both private and public sectors processing personal data. Transparency is required by Article 5(1)(a) GDPR (lawfulness, fairness and transparency principle) [*Article 4(1)(a) EUDPR*] and Articles 12 to 14 GDPR (transparent information requirements) [*Articles 14 to 16 EUDPR*], while human oversight is considered specifically in Article 22 GDPR [*Article 24 EUDPR*] and more broadly in Article 5(2) GDPR (accountability) [*Article 4(2) EUDPR*]. Therefore, this does not seem an issue for the EU's data protection legislation.

19. Certain AI applications, such as predictive policing[18] may have negative effects like over-policing on collectives, as well as on individuals. At the same time, data protection rules are designed to primarily protect individuals, and may not be well suited to address risks to *groups of individuals*. Since no specific individual is discriminated against if, for example, a neighbourhood slowly turns into a highly patrolled area, also anti-discrimination laws could be difficult to apply. The EDPS therefore recommends that any AI related regulation be designed to **protect from *any* negative impact**, not only on individuals, but also on collectives and society as a whole. On this regard, the EDPS invites the Commission to devise inclusive governance models which would empower organizations representing civil society (e.g. NGOs and other non-profit associations) so they also can help assessing the impact of AI applications on specific collectives and the society in general.

20. The EDPS agrees with the Commission that any future legal framework must consider elements regarding data quality and traceability, as well as transparency and human oversight and specific criteria for biometric identification systems. The EDPS fully supports these requirements, which correspond to some of the guiding principles laid down in the

[12] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57590

[13] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[14] "This requirement is closely linked with the principle of explicability and encompasses transparency of elements relevant to an AI system: the data, the system and the business models." HLEGAI Guidelines (page 18)

[15] "The data sets and the processes that yield the AI system's decision, including those of data gathering and data labelling as well as the algorithms used, should be documented to the best possible standard to allow for traceability and an increase in transparency. This also applies to the decisions made by the AI system. This enables identification of the reasons why an AI-decision was erroneous which, in turn, could help prevent future mistakes. Traceability facilitates auditability as well as explainability." HLEG Guidelines (page 18)

[16] "AI systems should support human autonomy and decision-making, as prescribed by the principle of respect for human autonomy." HLEG Guidelines (page 15)

[17] Feedback obtained from the public consultation on the guidelines published by the HLEG on AI.

[18] AI & Global Governance: Turning the Tide on Crime with Predictive Policing https://cpr.unu.edu/ai-global-governance-turning-the-tide-on-crime-with-predictive-policing.html

Declaration on ethics and data protection in AI, adopted by the 40th International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Brussels[19]. Moreover, the EDPS recommends considering also the other guiding principles laid down in the ICDPPC declaration, such as the responsible design and development by applying the principles of privacy by default and privacy by design and the individual's empowerment).

21. The EDPS acknowledges the recognition of the risks the use of AI may pose to a wide range of fundamental rights, including but clearly not limited to privacy and the protection of personal data[20]. The EDPS however submits that in addition increased surveillance and improper forms of governance (e.g. through machine learning classification and prediction, including of the behaviour of individuals, with or without facial recognition) should equally be considered as important risk factors for AI, e.g. because of their potential chilling effect on various other fundamental rights. Furthermore, while the White Paper identifies two sources of risks for the individuals – biased datasets and flawed AI system design – the EDPS considers that other risk sources should also be taken into account, including the lack of data quality, or risks stemming from the use of AI (such as the human tendency to trust in automated decision-making systems blindly[21]).

22. While the EDPS agrees that bias could also affect AI systems that learn during their operation, the White Paper goes further stating that when the AI system 'learns' while in operation '...the outcome *could not have been prevented or anticipated at the design phase*, the risks will not stem from a flaw in the original design of the system but rather from the practical impacts of the correlations or patterns that the system identifies in a large dataset.' (own emphasis). The EDPS disagrees with this assessment. **AI application design should take into account potential bias in the training data and, when applicable, in operational data.** Bias can and must be measured and corrected *during the operation* of AI applications as much as it can be measured and corrected during its development[22].

4. ASSESSMENT OF THE FUTURE REGULATORY FRAMEWORK FOR AI

4.1. Precautionary principle and risk-based approach

23. The White Paper follows a risk-based approach 'to help ensure that the regulatory intervention is proportionate', that is, to limit the applicability of the proposed regulatory framework. The White Paper proposition is to add certain legal requirements, complementary to the existing ones, for *high-risk* AI applications.

[19] https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_ai-declaration_adopted_en_0.pdfThe International Conference of Data Protection and Privacy Commissioners, now renamed Global Privacy Assembly, has been the premier global forum for data protection and privacy authorities for more than four decades.

[20] See also the paper from the Fundamental Rights Agency 'Facial recognition technology: fundamental rights considerations in the context of law enforcement', 27 November 2019, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf

[21] 'In fact, the supposedly reliable nature of AI mathematics-based solutions leads those taking decisions on the basis of the results of algorithms to believe the picture of individuals and society that analytics suggest. Moreover, this attitude may be reinforced by the risk of potential sanctions for taking a decision that ignores the results provided by analytics.' AI and data protection: Challenges and envisaged remedies. Report commissioned by the Council of Europe to Professor Alessandro Mantelero. https://rm.coe.int/report-on-artificial-intelligence-artificial-intelligence-and-data-pro/16808b2e39

[22] Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter?CMP=twt_a-technology_b-gdntech

24. In relation to the risks posed to data subjects by any AI applications processing personal data, such complementary regulation appears unnecessary, since the risk based approach already embodied in Articles 32 (security of processing) and 35 (Data Protection Impact Assessment) of the GDPR [*Articles 33 and 39 EDPR*] is seamless and must be adapted to the specific needs of each application. In February 2020, the EDPB concluded[23] 'that it is premature to revise the legislative text at this point in time'.

25. The White Paper's risk-based strategy states (p17): 'The mandatory requirements contained in the new regulatory framework on AI (see section D below) would in principle apply *only* to those applications identified as high-risk in accordance with [the] two *cumulative* criteria' of high-risk *sector* and of the *use and impact* of the AI application (own emphasis).

26. The EDPS suggests the following when and if a new regulatory framework were to be adopted:

27. <u>On the *cumulative* criteria for high risk</u>, the EDPS considers that the concept of 'high-risk' in the White Paper is too narrow, as it would seem to exclude individuals from being adequately protected from AI applications that could infringe on their fundamental rights. The White Paper acknowledges the lack of full coverage of the definition by stating 'there may also be exceptional instances where, due to the risks at stake, the use of AI applications for certain purposes is to be considered as high-risk'.

28. The EDPS is of the opinion that the approach to determining the level of risk the use of AI applications should be **more robust** and **more nuanced**, and European Data Protection Board's *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679*.[24]

29. With the precautionary principle in mind, the EDPS therefore recommends that the process determining high risk should be amended, when processing personal, data as follows:

    - To satisfy the 'harmful use and impact' criterion of the White Paper should compel the controller to conduct a data protection impact assessment in order to determine whether the AI application should be considered high-risk.

    - The criteria to determine the level of risk should reflect the European Data Protection Board's aforementioned Guidelines, and should therefore include: evaluation or scoring; automated-decision making with legal or similar significant effect; systematic monitoring; sensitive data; data processed on a large scale; datasets that have been matched or combined; data concerning vulnerable data subjects; innovative use or applying technological or organisational solutions; data transfer across borders outside the European Union; whether the processing in itself 'prevents data subjects from exercising a right or using a service or a contract.

[23] Contribution of the EDPB to the evaluation of the GDPR under Article 97 (p. 4)https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en

[24]The European Data Protection Board endorsed the Article 29 Working Party's 2017 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679 (wp248rev.01) during its first plenary meeting on 25 May 2018.https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

- Furthermore, the Commission should recognise that '[r]isks, which are related to potential negative impact on the data subject's rights, freedoms and interests, should be determined taking into consideration specific objective criteria such as the nature of personal data (e.g. sensitive or not), the category of data subject (e.g. minor or not), the number of data subjects affected, and the purpose of the processing. The severity and the likelihood of the impacts on rights and freedoms of the data subject constitute elements to take into consideration to evaluate the risks for individual's privacy.'[25]
- The 'sector' criterion referred to in the White Paper should serve not as a criterion, but instead as a presumptive indication that there is *by default* a need for an assessment (i.e. through a DPIA) of the risks raised by the AI application, and that any such risk might be even more serious than in another sector.

30. The White Paper's notion of risk of impact equally seems too narrowly defined. Beside 'the impact on the affected parties', the EDPS considers that the assessment of the level of risk of a given use of AI should also be based on **wider societal considerations**, including the impact on the democratic process, due process and the rule of law, the public interest, the potential for increased general surveillance, the environment[26] and (concentrations of) market power.

31. Regarding the impact specifically on individuals, the White Paper recognises the harm caused by AI may be both material and immaterial[27]. However, when it comes to the kind of harm taken into account to determine the (high) risk status, the White Paper considers a much narrower range of harms and risks[28]. When determining whether AI applications qualify as high-risk, the EDPS recommends the Commission not to limit itself to such narrow considerations and to rather consistently take into account the **very wide range of harms and risks faced by individuals.**

32. Additionally, while the White Paper recognises (p 11) that AI applications may generate risks because of 'flaws in the overall design of AI systems [...] or from the use of data without correcting possible bias,' the EDPS recommends that it also recognises that AI applications can also generate risks due to being partial or even arbitrary, misattributing variables, or failing to classify some data. It should furthermore recognise that risks can also arise from the *very act* of delegating tasks to machines (here, AI) which were previously assigned to humans. **The decision to 'solve' a societal problem using an AI application adds additional risks, which must be considered against any, purported increase in efficiency.**

For example, these systems require a huge amount of data which must be collected and stored, and this creates privacy and security risks; AI applications may not be able to take

[25] Article 29 Working Party 2014, *Statement on the role of a risk-based approach in data protection legal frameworks,* p4.

[26] The environmental impact of training an AI application, and that of using AI profusely might be detrimental to the EU's environmental targets:https://www.technologyreview.com/2019/06/06/239031/training-a-single-ai-model-can-emit-as-much-carbon-as-five-cars-in-their-lifetimes/

[27] 'both material (safety and health of individuals, including loss of life, damage to property) and immaterial (loss of privacy, limitations to the right of freedom of expression, human dignity, discrimination for instance in access to employment), and can relate to a wide variety of risks' White Paper, page 10

[28] 'Legal or similarly significant effects for the rights of an individual or a company; risk of injury, death or significant material or immaterial damage; effects that cannot reasonably be avoided by individuals or legal entities.' White Paper, page 17

into considerations human factors that do not transpire from the data; AI applications may benefit from human over-confidence and carry the appearance of objective truth or the aura of scientific reliability. Therefore, when the AI application processes personal data, there should be evidence of its necessity and proportionality[29].

33. On the new framework applying *only* to *high-risk* AI applications, the White Paper recognises the AI-*specific* risks and harms that may be brought about by AI applications (see top of p12). To address them, it proposes to update certain EU legislation, and, to the extent that not all the risks and harms would be covered by existing laws, to put forward AI-specific safeguards in a new 'regulatory framework for AI'.

34. However, the updates to EU legislation suggested in the White Paper (in section B) do not cover *all* these harms and risks, and the new safeguards put forward (in section D) only cover the risks caused by *high-risk* AI applications. In the EDPS' understanding, while the White Paper recognises a wide variety of risks and harms brought about by AI applications specifically, the measures it suggests would only address a portion of them, namely the category 'high risk'.

35. This approach does not reflect the precautionary approach taken by the European Union in personal data protection legislation.[30]The approach taken in the GDPR (and the EUDPR) is risk-based too, but, crucially, it is layered, whereas the AI White Paper seems to take an "all or nothing" approach:

    - The rules of the GDPR apply on the understanding that there is no such thing as a 'zero-risk' personal data processing operation. Every processing operation of personal data involves risks (though maybe minimal), especially automated processing, and especially through new technologies. Therefore, there is a certain number of obligations that should be fulfilled at any rate for all processing activities. *On top of that*, when risks go up (high risk), obligations increase too.

    - In contrast to that approach, the White Paper seems to propose that only high-risk AI applications require specific added obligations(additional to any obligations already applicable), and if risks go down, the added obligations disappear.

36. The precautionary principle as traditionally applied on the EU[31]demands precautionary measures whenever (1) unknown risks prove impossible to assess, or (2) there are grave risks but the probability of occurrence cannot be adequately foreseen. The precautionary principle in practice lowers the threshold for regulatory intervention (regulatory or other),[32] and its

[29] The underlying reason for implementing the AI system should be made clear and, in the case of cost-efficiency and effectiveness, well supported.

[30] See especially Article 29 Working Party 2014, Statement on the role of a risk-based approach in data protection legal frameworks, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

[31] The Precautionary principle is recognized by the Commission as applicable when "scientific evidence is insufficient, inconclusive or uncertain and there are indications through preliminary objective scientific evaluation that there are reasonable grounds for concern that the potentially dangerous effects (...) may be inconsistent with the chosen level of protection." See European Commission Communication on the Precautionary Principle (COM(2000)1 final), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0001&from=EN.

[32] Rather than bans, moratoria or phase-outs, precautionary actions may as readily take the form of strengthened standards, containment strategies, licensing arrangements, monitoring measures, labelling requirements, liability

application to the context of AI seems especially relevant.[33] The opinion of the EDPS is therefore that the risks and harms that *do not* satisfy the requirements to qualify as 'high risk' must *nonetheless* be avoided or mitigated, to the extent possible. To this end, the EDPS suggests that if the Commission were to put forward a new AI-specific regulatory framework, a certain number of reasonable safeguards should apply to *all* AI applications *regardless* of the level of risk, such as having technical and organizational measures in place (including documentation[34]) being be fully transparent about the goals, use, and design of algorithmic systems implemented;[35] ensuring the robustness of the AI system; or implementing and being transparent about the available mechanisms of accountability, redress and independent oversight.

37. While the Commission in its approach to AI aims at 'not being excessively prescriptive' so as to avoid creating 'a disproportionate burden, especially for SMEs' (p17), the result of such an approach might create a disproportionate burden on individuals' fundamental rights and interests instead. The EDPS suggests taking inspiration from the similar debate during the discussions and negotiations of the GDPR, and is of the opinion that the resulting **layered approach in the GDPR strikes a better balance between burdens and benefits**.

38. The EDPS further remarks that the protection of fundamental rights might warrant, in certain scenarios, not only specific safeguards but also a **clear limitation on the use of AI where certain uses of the technology are evidently incompatible with fundamental rights**.[36] The EDPS therefore suggests that some high-risk AI scenarios should be **forbidden from the outset**: following the European precautionary principle approach, and in particular when the impact on individuals and society as a whole is not yet fully understood, a temporary ban should be considered. The EDPS considers that these potential situations should be explicitly addressed in any possible future regulatory framework. The EDPS suggests to take over, in this regard, the 'cautious' and 'risk-adapted' approach proposed by the German Data Ethics Commission, by completely or partially banning algorithmic systems 'with an untenable potential for harm.'[37]

39. Besides any new requirements that the Commission might establish for AI applications, and in line with the UN Guiding Principles on Business and Human Rights, the Commission should also emphasise the **private sector's duty to exercise standard due diligence, and to take continuing, documented, proactive and reactive measures towards the protection of human rights**. Risk assessments, which make a lot of sense in technical environments where operators deals with their own operational risks, may not reflect the breadth needed when evaluating the impact on fundamental rights, and a data protection impact

provisions or compensation schemes. See Article 191(2) TFEU; cf. also Case C-180/96, United Kingdom v. Commission, 1998 E.C.R. I-2269, para. 99.

[33] The EDPS considers that this principle is applicable to the risks to privacy and to the protection of personal data, and therefore suggests considering its application concerning the risks posed by AI. See EDPS Guidelines on proportionality, footnote no. 53, at page 24: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

[34] Transparent documentation is an indispensable internal tool for controllers to manage accountability effectively and for ex-post control by DPAs as well as for the exercise of rights by data subjects. It goes beyond information to be given to the data subjects, and could increase protection until a fully-fledged ex-ante verification mechanism – and all the resources, know-how and political consensus it requires – materialises.

[35] Trade secrets and intellectual property rights are but a partial defence against transparency requirements and may be relied on only to the extent strictly necessary to protect the interests of their holders.

[36] The EDPS also suggests that ethical considerations should come into play regarding the use that is made of an AI application.

[37] https://datenethikkommission.de/wp-content/uploads/191023_DEK_Kurzfassung_en_bf.pdf

assessments(DPIA) (which also take into consideration rights other than the right to data protection, where relevant) is more appropriate.

4.2. Data Protection Impact Assessment

40. The DPIA provided for in Article 35 of the GDPR [*Article 39 EUDPR*] is a tool for **managing risks** to the rights and freedoms of the individuals. A DPIA is mandatory before processing data using innovative technologies if the processing is likely to result in high risk to the rights and freedoms of the individuals. The EDPS regrets that the White Paper does not explicitly mention DPIAs, despite its commitment to minimise the risks posed by AI 'on the application of rules designed to protect fundamental rights'.

41. The deployment of AI systems will most likely meet at least one of the criteria set in Article 35(3) GDPR [*Article 39 (3) EUDPR*][38]. Furthermore, Article 35(4) GDPR [*Article 39(4) EUDPR*] allows the data protection supervisory authorities of each EU Member State (and the EDPS) to publish a list of the kind of processing operations, which are subject to the requirement for a DPIA. The EDPB published further guidance on determining when carrying out a DPIA is mandatory[39]. Among others, the supervisory authorities of Poland, Italy, Greece, Austria and the Czech Republic require a DPIA for some or all uses of AI applications. (e.g. in Poland a DPIA is required for 'creditworthiness assessment, with the use of AI algorithms' while in the Czech Republic such a DPIA is required for 'automated expert systems including AI' when used for analysis or profiling IT AI systems).

42. Article 35 GDPR [*Article 39 EUDPR]* refers to a likely high risk "to the rights and freedoms of individuals". 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]

43. It is important to note that the GDPR's requirements for a DPIA including not only a risk assessment, but also a detailed description of the envisaged data processing. The risk assessment part is about identifying the risks and the measures to address and mitigate those risks. The risks need to be measured against each other and given a value or score that makes them scalable. This value should be based on the likelihood and severity of the risks. The description of the envisaged data processing should entail the scope, nature, context, and purposes of the data processing.

44. The DPIA equally requires further an **assessment of necessity and proportionality** of the processing. The necessity assessment should demonstrate that the deployment of AI is indeed the most suitable tool for fulfilling the goal of a specific data processing activity. If

[38] Data processing activities fall under the obligation to produce a DPIA if (1) there is a systematic and extensive evaluation of personal data based on automated processing, including profiling, and on which decisions are based that will result in legal or similarly significant effects (2) the processing involves large scale of sensitive data or data related to criminal convictions and offenses, or (3) the processing involves systematic monitoring of publicly accessible areas on large scale.

[39] The Article 29 Working Party adopted a document „Guidance on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in high risk" for the purposes of Regulation (EU) 2016/679 that contains detailed guidelines how and when a DPIA should be carried out.

[40] European Data Protection Board, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01.

there are other less intrusive methods with lower level of potential risks that could help achieve the purpose of the processing just as well, specific arguments are needed to show why the data controller opted for using AI instead.

The proportionality assessment should take into account a number of factors, in particular:

- the data controllers' interest and the rights and freedoms of the individuals and
- the reasonable expectations of the individuals and the purpose of the data processing.

The EDPS points out that if the data protection impact assessment shows that the processing would entail a high risk for the rights and freedoms of the data subjects, unless the data controller takes measures to mitigate the risk, there is an obligation to consult the supervisory authority under Article 36 (1) GDPR [*Article 40 EUDPR]*.**The EDPS therefore suggests that a future legal framework should lay down the requirement of an impact assessment for *any* envisaged deployment of AI systems.** Where this involves the processing of personal data, the requirements of the GDPR for the DPIA must be met; for other situations, the proposed AI Impact Assessment could include the following main components:

1. Identifying the concerned fundamental rights
    a. What are the affected or potentially affected fundamental rights?
    b. What is the nature of these fundamental rights? Is an absolute right affected?
2. Identifying the risks to those rights during the development and during the deployment phase
    a. What are the risk factors?
    b. What is the likelihood of the risks to manifest?
    c. To what extent would the risks have an impact on the fundamental rights?
3. Identifying the measures to mitigate the affected rights
    a. What methods, technical or organisational are at disposal to guarantee that the core of the fundamental rights will not be affected?
4. Balancing of interests and risks
    a. What are the positive/negative impacts of the limitation on the fundamental rights?
    b. What are the positive/negative impacts of the processing for the individual?[41]

The EDPS is of the opinion that introducing such an assessment of risk is in line with the Commission's strategy to better implement the Charter of the Fundamental Rights by the

[41] See Heleen L. Janssen, *'An approach for a fundamental rights impact assessment to automated decision-making'* International Data Privacy Law, Volume 10, Issue 1, February 2020, Pages 76–106, https://doi.org/10.1093/idpl/ipz028.

European Union.[42] Therefore, while it is not a completely new idea as such, its application should be considered for the processing of personal data using AI, given the serious impact and innovative nature of the technology.

45. Finally, the EDPS recommends, whenever possible, **making public** the results of such assessments, or at least the main findings and conclusions of the DPIA, as a trust and transparency enhancing measure.

4.3. Accountability and enforcement

46. On page 10, the White Paper states that 'some specific features of AI (e.g. opacity) can make the application and enforcement of this legislation more difficult'. According to the paper, such enforcement difficulties would require 'to examine whether current legislation is able to address the risks of AI and can be effectively enforced, whether adaptations of the legislation are needed, or whether new legislation is needed'.

47. On page 12, the White Paper further elaborates the problematic features present on many AI applications listing among them the 'opacity ('black box-effect'), complexity, unpredictability and partially autonomous behaviour' and specifying that they '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.' However, such features are not exclusive to AI applications. For instance, processing of personal data through Big Data techniques can be as complex, and some applications that do not use AI (e.g. those managing automated trains[43]) are partially or fully autonomous.

48. The opacity attributed to some types of AI applications relates to the human incapacity to explain the reasoning behind the AI application decision. Such a problem stems from the way in which those applications represent the knowledge and experience they use to make decisions. The EDPS therefore suggests that **transparent test and audit procedures,** mentioned in section 5.F in the context of prior conformity assessments, should be part of any AI application processing personal data. Making such procedures publicly available would ensure that supervisory authorities could perform their tasks, but also improve user trust in the AI applications.

49. If, as the White Paper suggests, opacity or other features specific to AI require the review of existing legislation, **the EDPS stresses the need for a sound regulatory gap analysis in the impact assessments** as required by the Commission's better regulation guidelines[44] and the Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making[45]. Such analysis would describe the relevant AI features, the gaps of the current legislation that need amendment and the approach of the proposed amendments to fill in such gaps.

[42] EC Communication *'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union*' COM (2010) 573 FINAL, Brussels, 19.10.2010.
[43]https://en.wikipedia.org/wiki/List_of_automated_train_systems
[44]https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox_en
[45] OJ L 123, 12.5.2016, p. 1–14.

50. The White Paper puts into question whether competent authorities and affected individuals could 'verify how a given decision made with the involvement of AI was taken and, therefore, whether the relevant rules were respected'. The EDPS would like to recall the principle of accountability underpinning the GDPR, according to which it is the data controller who must demonstrate compliance with the GDPR. Claims made about the lack of human (or any other) discriminatory bias in AI application should be verifiable[46].

51. The White Paper expresses concerns[47] on the supervisory authorities' potential lack of means to enforce existing regulation on AI. The EDPS shares those concerns and underlines the necessity of providing supervisory authorities with the resources to keep up not only with AI, but also with any technological developments[48].**The EDPB evaluation of the GDPR showed[49] that most DPAs considered their 'resources from a human, financial and technical point of view' were not sufficient.** Cooperation and joint investigations between all relevant oversight bodies, including data protection supervisory authorities, should be encouraged.

52. The White Paper mentions (p. 14) that 'The lack of transparency (opaqueness of AI) makes it difficult to identify and prove possible breaches of laws, including legal provisions that protect fundamental rights, attribute liability and meet the conditions to claim compensation.' The EDPS is of the view that transparency in AI applications goes beyond intelligibility and includes providing users clear information on the use of AI systems.

4.4. Regulatory requirements

53. The EDPS welcomes the list of regulatory requirements included in section 5.D, which mostly overlap with existing data protection legislation and the aforementioned **Declaration on ethics and data protection in AI**. However, he considers that requirements like lack of unfair discrimination, or robustness and accuracy are so fundamental that they should apply to any AI application, not just to 'high risk' AI applications.

54. The EDPS is of the view that most of the requirements described in section 5.D, like 'Robustness and accuracy' or 'clearly inform individuals when they are interacting with an AI application and not a human being' are covered by existing data protection rules. The EDPS welcomes the approach of the human oversight requirement, which is in line with the individual empowerment foreseen in the aforementioned **ICDPPC Declaration on ethics and data protection in AI** and goes further than the requirements of Article 22 GDPR (automated individual decision making, including profiling) [*Article 24 EUDPR*].

55. The EDPS agrees with the relevance of the requirement of information provision. Nevertheless, appropriate granularity of information will be different in different contexts.

[46] For example, in November 2019 a prominent software developer claimed Apple Credit card was "sexist" against women applying for credit. The AI system complexity did not allow the credit entity to demonstrate its fairness. The New York State Department of Financial Services is investigating the case. https://www.nytimes.com/2019/11/10/business/Apple-credit-card-investigation.html

[47] '...enforcement authorities may find themselves in a situation where they [...] don't have the appropriate technical capabilities for inspecting systems.'

[48] A report published in April 2020 assessed the technical staff and budget of Data Protection authorities in the EU since the GDPR came into force and criticized the development of their technical enforcement capacity.

[49] Contribution of the EDPB to the evaluation of the GDPR under Article 97 (p. 30) https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en

Therefore, the EDPS recommends **developing informational standards** aimed at harmonizing the information provided to individuals for different types of AI applications.

4.5. Controls and governance

56. Section 5.F of the White Paper proposes an objective prior conformity assessment mandatory for high-risk AI systems. The European Commission defines[50] conformity assessments as risk analysis ensuring that products comply with certain rules before placing them on the market, carried out during the design and production phase.

57. On the one hand, the prior conformity assessment would check the compliance with the regulatory requirements described in section 5.D. On the other hand, a DPIA (which would be mandatory for high-risk AI applications in accordance with the GDPR) would assist the controller to check the compliance with the GDPR. The EDPS observes a potential conflict between those two checks, due to the overlap between their requirement sets. Diverging conclusions on each check for an AI application would create confusion and legal uncertainty, and should therefore be avoided. The EDPS therefore recommends the Commission to ensure that the possible future regulatory framework would not create overlap among supervisory authorities and to include a cooperation mechanism between such authorities.

58. The White Paper asks for the establishment of similar conformity mechanisms '*Where no such existing mechanisms can be* relied *on*', but it does not clarify which would be the competent authorities involved in such conformity mechanism. If the European Commission were to follow the call for the establishment of a European Agency for AI[51], it is unclear how to avoid a competency overlap.

59. Section 5. G proposes a voluntary labelling scheme for those AI systems not classified as high-risk. This label would be used for those committing to fulfil the regulatory requirements in section 5.D or a specific set of similar requirements especially established for the purposes of such labelling scheme. However, AI lacks standards allowing the AI application developers consistently check their compliance. Without such standards, the value of the voluntary labelling scheme would be limited at best.

60. The EDPS welcomes the mention to the *ex post* enforcement and compliance monitoring by competent authorities. However, such controls should not be limited to checking documentation and testing the applications. Other aspects, such as checking transparency (including the capacity to explain how it reaches decisions) and the tests performed on the training data to ensure their adequacy, could also be necessary.

61. The EDPS fully supports the objectives defined by the White Paper for a European governance structure on AI ('*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.')*. It will be crucial that, as mentioned later in the paper, such structure avoids duplicating the already existing

[50] https://europa.eu/youreurope/business/product-requirements/compliance/conformity-assessment/index_en.htm

[51] European Parliament, Committee on Legal Affairs, Draft report with recommendations to the Commission on a framework of ethical aspects of AI, robotics and related technologies. https://www.europarl.europa.eu/doceo/document/JURI-PR-650508_EN.pdf

functions, and that it involves the existing EU-level authorities, such as the European Data Protection Board.

5. OTHER SPECIFIC ISSUES

5.1. Remote biometric identification

62. The White Paper recognises the risks for fundamental rights brought about by Remote Biometric Identification (RBI), an observation shared by the EDPS. Remote Biometric Identification raises two issues: the (distant, scalable and sometimes covert) identification of individuals, and the (distant, scalable and sometimes covert) processing of their biometric data. Technologies related to either of these two features, whether or not they rely on AI, may be similarly problematic and may need to fall under the same limitations as RBI.

63. The risks posed to the rights and freedoms of individuals by RBI systems, such as live facial recognition in public places, must be properly identified and mitigated, and such a process should involve those most impacted by the use of such technology. Some of the risks of RBI come from the fact that RBI systems are easily hidden, frictionless, often are presented as mere “experiment” but could easily be turned into ubiquitous and pervasive surveillance complex.

64. Once the infrastructure supporting RBI is in place, it may easily be used for other purposes (‘function creep’). Some have recently claimed that RBI systems, or parts of other technical infrastructures, could be used to fight the ongoing pandemic in different ways, such as through the measurement of social distancing or of the use of masks, or temperature checks (when cameras have integrated thermometers). Some of these new applications may not fall under the scope of the GDPR, but would nonetheless have a chilling effect in democratic societies. Such uses of AI, and such function creeps, should therefore be properly addressed in any regulation on AI.

65. While RBI may pose serious fundamental rights challenges, the EDPS would like to highlight that RBI-related technologies which do not aim at the identification of the individual raise serious privacy concerns too: for example, the detection of emotions – based on real time facial recognition –can infer feelings of individuals[52].

66. It is of the utmost importance to assess whether the technology is necessary or proportional in the relevant situation where it will be deployed – or if it is even desired[53]. To this end, the EDPS supports the idea of a **moratorium on the deployment, in the EU, of automated recognition in public spaces of human features**, not only of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, so that an informed and democratic debate can take place and until the moment when the EU and Member States have all the appropriate safeguards, including a comprehensive legal framework in place to guarantee the proportionality of the respective technologies and systems for the specific use case.

[52] Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements https://journals.sagepub.com/stoken/default+domain/10.1177%2F1529100619832930-FREE/pdf

[53] A 2020 study by the European Union Agency for Fundamental Rights demonstrated that **over 80% of Europeans are against sharing their facial data with authorities**.

67. The **use of RBI by public authorities** during times of national emergency, such as during a cross-border or national health crisis, **should always be necessary for reasons of substantial public interest, on the basis of Union or Member State law, transparent, accountable, proportionate** to the aim pursued**, subject to specific safeguards, clearly limited in time and compatible with the essence of fundamental rights and the respect of human dignity**.

5.2. Vulnerable groups

68. The EDPS welcomes the fact that the Commission recognises the specific risks AI applications tend to impose on vulnerable group of persons. However, the White Paper considers these risks explicitly only in relation to 'the rights to respect for private life and protection of personal data at the core of fundamental rights concerns when using facial recognition technology' where there is 'a potential impact on non-discrimination and rights of special groups, such as children, older persons and persons with disabilities'.

69. First, in the absence of a formally adopted legal definition of vulnerable groups, the EDPS suggests a **context-specific, pragmatic approach**. Vulnerable group of persons should include children, elderly, and persons with disabilities, ethnic minorities or historically marginalised groups, women, LGBTQIA+ communities, workers and others at risk of exclusion.

70. Furthermore, the EDPS considers that the issue of vulnerable groups should **not only be considered in the context of remote biometric identification systems**, but in a much broader context. The EDPS highlights that AI systems should be fair and respectful to the human dignity and to the rights and freedoms of the individuals. In the context of vulnerable groups, fairness implies **non-discrimination**. Willing and unwilling discrimination is an inherent attribute of human decision-making, and if not acting carefully, AI systems may reflect this natural human bias. As the White Paper rightfully states, 'the same bias when present in AI could have a much larger effect, affecting and discriminating many people'. This may result in direct and indirect ramifications in many aspects of life, such as social, economic and health aspects.

71. In any event, where such AI application occurs, there is a high risk of tangible (material damage to property, quantifiable loss) and non-tangible (loss of privacy, limitations to the right of human dignity) harm. Therefore, the special interests of vulnerable groups should be taken into account in any situation similar to the abovementioned list. The EDPS encourages the Commission to provide a non-exhaustive list of AI applications from various sectors and for various purposes that may endanger the right to equal treatment and to non-discrimination as stated in Article 20 and 21 of the Charter of Fundamental Rights of the European Union.

72. The EDPS suggests that in order to avoid such adverse effects, vulnerable groups should be considered both while developing and using AI. Even at the early stages, when training AI systems, special attention should be given to vulnerable groups, since most of the time the inaccuracies of AI arise from incorrect labelling of training data or non-representative data sets. As the White Paper states, **requirements** could be envisaged 'to take reasonable measures aimed at ensuring that such subsequent use of AI systems does not lead to outcomes entailing prohibited discrimination. These requirements could entail in particular obligations to use data sets that are sufficiently representative, especially, to ensure that all

relevant dimensions of gender, ethnicity and other possible grounds of prohibited discrimination are appropriately reflected in those data sets'. Such measures could include for example requirement on entry level to assess data quality, possibility of human oversight, redress or a 'right to explanation' where the deployment of AI lead to negative impact for the individual, similar to the provisions of Article 22 (4) GDPR on automated decision-making and profiling.

5.3. Access to data

73. The White Paper signals edge computing as a relevant trend in the evolution and development of AI. This view is consistent with the one expressed in the European Commission's Data Strategy. However, neither the White Paper nor the Data Strategy explain how closer physical data location would translate into improved data availability or AI trustworthiness.

74. While the location of data may have legal consequences (e.g. applicable law or rules applicable to international transfers of personal data), data availability does not depend on their physical location but on the technical controls to access to them (e.g. through Application Program Interfaces and data exchange formats). Data close to users (e.g. data stored in a smart watch) could be inaccessible for them unless there is an API or other technical means allowing accessing those data. On the other hand, data stored in a private cloud thousands of kilometres away could be ready at hand, if the cloud storage is easily accessible for its users.

75. The EDPS is of the view that the Commission should foster the development and adoption of standardized Application Program Interfaces[54] (API). The adoption of such APIs would ease the access to the data for the authorised users independently of the location of that data and would be a driver for data portability.

76. The EDPS stresses that the EU regulatory framework should apply to datasets published outside EU, but used in the EU. AI applications developed or used by the European public sector or by companies cannot rely on datasets not compliant with EU data protection legislation or being contrary to EU values and fundamental rights.

6. CONCLUSIONS

77. The EDPS fully agrees with the Commissions in the need of a European approach to AI and very much welcomes in this regard the White Paper's commitment to fundamental rights and European values.

78. However, the EDPS is of the view that the proposals set out in the White Paper need further adjustments and clarifications in some relevant questions. Among the topics that would require more clarity in any future legislative proposal are the link between the risks posed by AI and the related legislative gaps, the risk-based approach applied to AI applications and the definition of AI itself that should allow clearly defining the scope of the proposed legislation.

[54] Credit institutions are developing APIs to ensure 'objective, non-discriminatory and proportionate' access to financial data as required by the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market

79. The EDPS recommends in addition that any new regulatory framework for AI:

- **applies both** to EU Member States and to EU institutions, offices, bodies and agencies;

- is designed to **protect from any negative impact**, not only on individuals, but also on communities and society as a whole;

- proposes **a more robust and nuanced risk classification scheme**, ensuring any significant potential harm posed by AI applications is matched by appropriate mitigating measures;

- includes an impact assessment **clearly defining the regulatory gaps** that it intends to fill.

- **avoids overlap** of different supervisory authorities and includes a cooperation mechanism.

80. Regarding remote biometric identification, the EDPS supports the idea of **a moratorium on the deployment, in the EU, of automated recognition in public spaces of human features**, not only of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, so that an informed and democratic debate can take place and until the moment when the EU and Member States have all the appropriate safeguards, including a comprehensive legal framework in place to guarantee the proportionality of the respective technologies and systems for the specific use case.

81. If there would be a new legal framework as reflected in the White Paper and the Commission's Work Programme, the EDPS will provide further advice to the Commission as foreseen in Article 42 of the EUDPR.

Brussels, 29 June 2020

Wojciech Rafał WIEWIÓROWSKI