INFINITY

IMMERSE. INTERACT. INVESTIGATE.

Policy Brief

Legal, ethical and societal frameworks

DISSEMINATION LEVEL PUBLIC

PARTNER

UNIVERSITY OF VIENNA

AUTHORS

Thomas Por

Max Königseder

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883293. The content of this document represents the view of the authors only and is their sole responsibility. The European Commission does not accept any responsibilty for any use that may be made of the information it contains.

Legal,ethical and societal frameworks

1. The upcoming AI Regulation and its implications for law enforcemnt

On April 21st, the European Commission proposed the first-ever comprehensive legal framework laying down harmonised rules on artificial intelligence: the Artificial Intelligence Act.[1] This first draft is the outcome of a consultation process that started in 2018 when the EC first outlined its 'European Approach to AI'. The aim of the proposed Regulation itself is in the tradition of previous regulatory approaches of emerging technologies: fostering innovation and uptake of economic and societal benefits while mitigating the risks and protecting fundamental rights. Whether the regulation will be able to meet these ambitious goals and provide a world-wide gold standard for AI regulation remains to be seen. In any case, the development of this regulation will significantly set the course for production and deployment of AI-featured software across numerous sectors, including law enforcement and the prevention, detection and investigation of criminal offences. Therefore, in the midst of this legislative process, it is important to understand and reflect upon how we got here, where we stand and where we want to go?

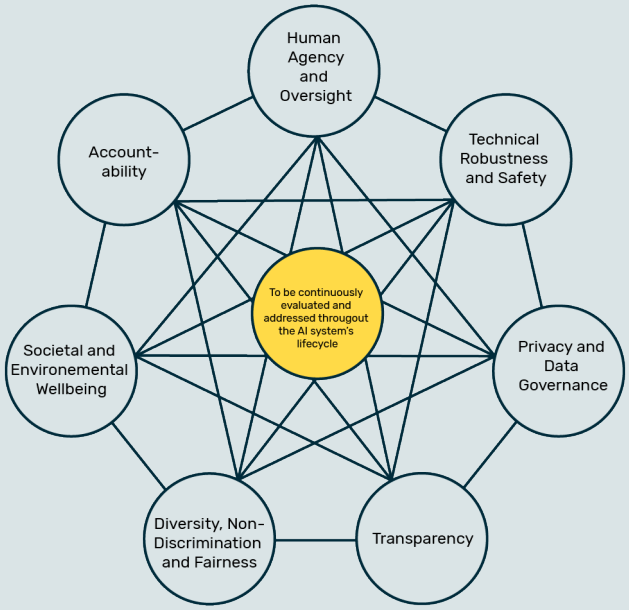
Key Terms

ADM	Automated Decision Making	EDPS	European Data Protection Supervisor
AI	Artificial Intelligence	EU	European Union
AI HLEG	AI High Level Expert Group	GDPR	General Data Protection Regulation
CIPL	Centre for Information Policy Leadership	ICO	Information Commissioner's Office
DPIA	Data Protection Impact Assessment	LED	Law Enforcement Directive
DPO	Data Protection Officer	LIBE	Committee on Civil Liberties, Justice and Home Affairs
EC	European Commission		
EDPB	European Data Protection Board	MS	(EU) Member State

2. How did we get there? The chrononolgy of the AI Regulation

Embedding AI technologies into existing legal frameworks is a policy challenge in jurisdictions globally. Multiple institutions and stakeholders on national and supranational level have issued opinions, guidelines and resolutions. Most prominently, at the EU level, the High-Level Expert Group on Artificial Intelligence has produced Ethics Guidelines for Trustworthy AI. In order to maintain social control over the technology, the guidelines provide three essential components (lawful, ethical and robust) and seven key requirements that AI systems should meet to be deemed trustworthy.

Human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; and accountability.[2]



Seven key requirements of AI (AI HLEG)

These ethical guidelines are of particular relevance, since they helped frame the ongoing discussions and structured the debate for the next phases of legislative action: The White Paper on Artificial Intelligence – A European approach to excellence and trust.[3] In February 2021, the EC published its long-awaited white book on AI regulation. Hereby the Commission initiated a consultation of Member States civil society, industry and academics.[4] The Commission announced an upcoming regulatory action, presented the key elements of such a future framework and officially started the European legislative process.

The White Paper consists of two main building blocks, an 'ecosystem of excellence' and an 'ecosystem of trust'. The latter outlines the EU's approach for a regulatory framework for AI. The Commission introduced a risk-based approach that differentiates between 'high-risk' and 'non-high-risk' AI applications. Only the former should be in the scope of a future EU regulatory framework. At this point it could already be anticipated that, considering sector and use of the deployment and the human rights sensitivity of law enforcement operations, the deployment of AI by law enforcement agencies will fall under the umbrella of high-risk AI. The White Paper introduced six key requirements for high-risk AI applications, that could become legal obligations in the future: Training data, data and record-keeping, provision of information, robustness and accuracy, human oversight and specific requirements for certain AI applications, such as remote biometric identification.[5]

As a result of this three-year process, in which a broad range of stakeholders had the chance to make their voices heard, the European Commission proposed a legal framework to regulate AI. This first proposal for a draft legislation by the Commission was unveiled in April 2021 and brought a fine-tuning of the 2020 risk-based approach. This is where we stand in October 2021.

3. Where do we stand?

3.1 The draft proposal

As mentioned above, the European Commission recently presented its '*new rules and actions aiming to turn Europe into the global hub for trustworthy Artificial Intelligence (AI)*'.[6] In this context, it also published the first '*Proposal for a Regulation laying down harmonised rules on artificial intelligence*'.[7] Even though the proposal is not legally binding and will most likely be subject to changes and amendments in the legislative process, it is still worth taking a look in which direction the regulation of AI algorithms might go in Europe. Especially for AI based projects such as INFINITY. The following section will give a short overview of the Proposal by

the Commission.

The EC's approach to an AI regulation is to embrace the possibilities this technology brings, while managing the risks of AI applications. First, an *"artificial intelligence system (AI system)"* is defined as a "*software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*".[8] The Commission refers to the different annexes in several cases, because this allows adapting the regulation to new technological innovations quicker and less bureaucratically. At the moment, the Commission has included the following techniques in Annex I:

- *Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;*
- *Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;*
- *Statistical approaches, Bayesian estimation, search and optimization methods.*

Second, the Commission suggested a **risk-based approach**. If such an AI system is provided within the scope of Article 2 of the Regulation, different rules shall apply based on the risks associated with the specific system. The Commission distinguishes between systems, which are considered unacceptable risks, high risks, limited risks or minimal risks. The first two categories will be presented below, as they are mainly of relevance for law enforcement activities.

3.1.1 Unacceptable risk?

AI systems of the first category are considered a clear threat to the safety, livelihoods and rights of people and shall be banned. This includes AI systems or applications that manipulate human behaviour to circumvent users' free will and systems that allow 'social scoring' by governments. [9]

Especially relevant to law enforcement activities is the prohibition of Article 5(1)(d) of the Proposal: ['The following artificial intelligence practices shall be prohibited'...] *"the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives..."*.[10]

As the term 'unless' is indicating, the aforementioned is not an absolute prohibition of real-time identification and tracking techniques in public places. Such surveillance systems could be used lawfully, if

- the targeted search for specific potential victims of crime, including missing children;
- the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;
- the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA62 and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.

Article 5(2-4) include additional conditions which have to be adhered to in order to enable the lawful "*use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement*".[11]

3.1.2 High risk AI systems

Most AI systems developed for law enforcement activities will be considered high risk pursuant to Article 6(2). This provision is referring to Annex III, which includes the following section on AI systems intended to be used by law enforcement agencies.

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas related to law enforcement

- AI systems intended to be used by law enforcement authorities f**or making individual risk assessments of natural persons** in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;
- AI systems intended to be used by law enforcement authorities as **polygraphs and similar tools** or to **detect the emotional state** of a natural person;
- AI systems intended to be used by law enforcement authorities to **detect deep fakes** as referred to in article 52(3);
- AI systems intended to be used by law enforcement authorities for **evaluation of the reliability of evidence** in the course of investigation or prosecution of criminal offences;
- AI systems intended to be used by law enforcement authorities for p**redicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons** as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;
- AI systems intended to be used by law enforcement authorities for **profiling of natural persons** as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;
- AI systems intended to be used for **crime analytics regarding natural persons**, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data

3.1.3 Data and data governance

A key factor for the reliability and proper functioning of AI systems – especially important if they are considered high risk – is the data the AI systems are trained, validated and tested with. Biased, incomplete or incorrect data could have a severe impact on the output of the algorithms and could lead to discriminatory and/or false results. Therefore, the proposed AI regulation introduces data quality criteria which AI systems have to fulfil. Article 10(2-5) of the proposed AI Regulation regulates the data governance for high-risk AI systems:

Article 10 Proposal Artificial Intelligence Act

2. Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular,

- *a) the relevant design choices;*

» *b) data collection;*

» *c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation;*

» *d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;*

» *e) a prior assessment of the availability, quantity and suitability of the data sets that are needed;*

» *f) examination in view of possible biases;*

» *g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed.*

3. Training, validation and testing data sets shall be relevant, representative, free of errors and complete. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. These characteristics of the data sets may be met at the level of individual data sets or a combination thereof.

4. Training, validation and testing data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the highrisk AI system is intended to be used.

5. To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

3.1.4 Additional safeguards

Following the risk-based approach of the Proposal, different safeguards will be introduced dependent from the respective level of risk. High-risk AI systems will be subject to strict obligations before they can be put on the market, such as:

» Adequate risk assessment and mitigation systems;

» High quality of the datasets feeding the system to minimise risks and discriminatory outcomes;

» Logging of activity to ensure traceability of results;

» Detailed documentation providing all information necessary on the system and its purpose for authorities to assess its compliance;

» Clear and adequate information to the user;

» Appropriate human oversight measures to minimise risk;

» High level of robustness, security and accuracy.[12]

3.2 De lege lata (*the law as it exists*)

De lege lata there is no comprehensive European legal framework covering Artificial Intelligence in force within the EU. Even though, a comprehensive legal framework is yet to be established we do not find ourselves in a legal vacuum. Quite the opposite is the case. Developers and deployers of AI are already subject to European and national legislation ranging from consumer protection, product safety and liability and fundamental rights (first and foremost data protection, privacy and non-discrimination). The so-called 'European approach to AI'[13] must be grounded in EU values and fundamental rights ranging from human dignity, equality, the rule of law, pluralism, due process and especially the protection of privacy and personal data and therefore respect the European data protection acquis in its entirety. The General Data Protection Regulation 2016/679 (GDPR) has been developed as a technology neutral legislation that is capable of responding to new, evolving and emerging technologies such as AI. It is apparent that Artificial Intelligence requires access to big data, including the use of personal

data in terms of the GDPR and corresponding legislation, most notably the Law Enforcement Directive. The EDPB has emphasised the self-evident fact that '*any processing of personal data through an algorithm falls within the scope of the GDPR.*'[14] Therefore the entirety of European data protection legislation needs to be adhered at every point of development and deployment (depending on the purpose the LED, the sibling of the GPDR applies to LEAs). Some GDPR provisions and considerations are of special relevance and will be reiterated and further analysed in the following subsection.

3.2.1 AI and data protection

Obviously, even though the requirements that were developed so far in the European legislative process are not limited to data privacy and aim to address a broader set of concerns arising from this technology, they overlap in various ways and are strongly influenced by the concepts and requirements of European Data Protection legislation such as the GDPR or the LED. The following selected problems are intended to illustrate the significance of this overlap.

Profiling and automated decision-making

The GDPR (Art 22) as well as Directive 2016/680 (Art 11) prohibit automated individual decisions that are made without human involvement or intervention in the decision-making process ('solely automated decision-making'). Due to the inherent differences in the scope of application of the two instruments, the prohibitions for ADM and profiling are not identical despite some similarities. Art 22(1) GDPR for examples introduces three possible exceptions from the general ban:

- *is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
- *is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or*
- *is based on the data subject's explicit consent.*[15]

Art. 11(1) of the Directive states that profiling produces an adverse legal effect concerning the data subject or significantly affects him or her and should therefore be prohibited unless authorised by Union or MS law to which a controller is subject and which provides appropriate safeguards for the rights of freedoms of the data subject.[16]

In Art. 11(3) the Directive explicitly prohibits profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Art 10 of the Directive, in accordance with Union law.[17]

The former Article 29 Working Party has already provided guidelines on automated individual decision-making and profiling in the scope of the GDPR.[18] However, the FRA believes that the concept of automated decision making is elusive and therefore requires further discussion and research.[19] The applicability of this provision might not even be of relevance since the intended use of AI will only be developed to assist the investigator in the decision-making process. The human intervention has to suffice the requirement of being qualified, capable of discovering and recovering unfair outcomes or discriminations, as the European Data Protection Board (EDPB) has recently pointed out in its guidelines on data protection by design and by default.[20]

Data minimisation

The tension between the principle of data minimisation and the fact, that algorithms need to be trained by a substantial amount of data to be efficient, may seem apparent. AI systems may not be able to perform without first being trained on large data sets. Additionally, simply maximizing the amounts of data to feed into the algorithm entails to increases the risk of possibly unlawful data collection practices, especially regarding secondary processing. However, the concepts of Big Data and Machine Learning are not incompatible with the principle of Data Minimisation. The principle itself does not limit the processing of data by way of reference to a specific volume or set of data elements, but it refers to what is 'necessary' for the purposes of the processing. What personal data is considered 'necessary' varies depending on the AI system and the objective for which it is used. The level of accuracy that is required is to be a determining factor in the selection of data elements for inclusion. Additionally, as best practices it was suggested

that controllers should set limits that are sufficient to achieve the purpose of the processing, rather than using all available data.[21]

Data protection impact assessments (DPIA)

Art. 35 GDPR provides the concept of a Data Protection Impact Assessment:

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, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*

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 as this was also reiterated by the European Data Protection Supervisor (EDPS) opinion on the AI White Paper.[22]

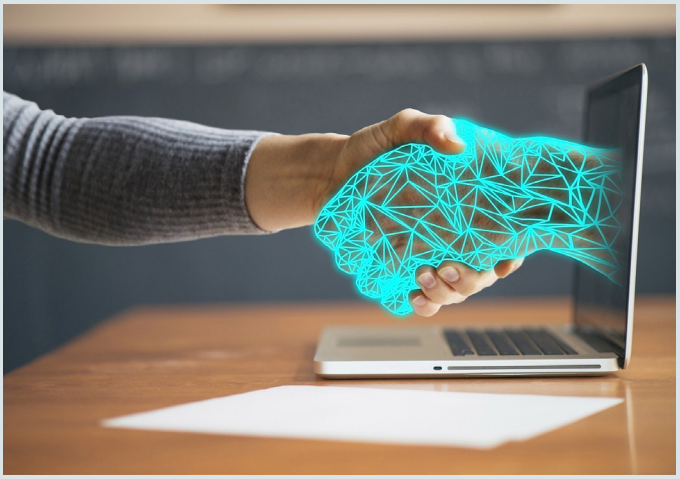
The Art 29 Working Party considers a Data Protection Impact Assessment (DPIA) as a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. In other words, a DPIA is a process for building and demonstrating compliance.[23]

A DPIA can be considered necessary if for example the processing could affect a large number of data subjects and is likely to result in a high risk to the rights and freedoms of the data subject, especially when using new technologies. The use or development of an algorithm can trigger the obligation to carry out a DPIA prior to any processing taking place. The U.K. Information Commissioner's Office (ICO) highlights that AI, machine learning and deep learning are to be considered as innovative technologies that likely trigger the requirement for a DPIA in terms of Article 35 GDPR.[24] Even in cases where the GDPR does not require the controller to conduct a DPIA, it is good practice to conduct such an assessment in order to ascertain and minimise risk wherever the envisaged data processing is complex, large-scale or sensitive.

If the outcome of the DPIA indicates that the processing would, in the absence of measures, result in a high risk, the controller will have to consult the relevant supervisory authority prior to the processing. The outcome of the assessment can also be that the controller will have to refrain from using a specific algorithm, or parts of it, if the risks to the rights of data subjects and other persons cannot be sufficiently mitigated.

Overlap between the concepts of data protection and trustworthy AI

The Centre for Information Policy Leadership (CIPL) has developed a table in its report that shows the overlap between the seven key requirements of the AI HLEG Guidelines and the requirements of the GDPR. The table exemplifies the extent to which GDPR concepts have inspired the principles of trustworthy AI and will likely shape the upcoming AI Regulation as outlined above.



Key requirements of Trustworthy AI	Overlap with GDPR provision
Human Agency and Oversight	» Legitimate interest balancing test (Art. 6(1)(f)) » Transparency (Art. 13 & 14) » ADM (Art. 22) and right to obtain human intervention (Art. 22(3)) » Risk assessment and DPIA (Art. 35)
Technical Robustness and Safety	» Security (Art. 32) » Risk assessment and DPIA (Art. 35) » Data accuracy (Art. 5(1)(d))
Privacy and Data Governance	» Data protection principles (Art. 5) » Legal grounds for processing (Art. 6) » Legal grounds for sensitive data (Art. 9) » Rights of the data subject (Chapter III) and in particular Transparency (Art. 13 & 14); Right to information on ADM and logic involved (Art. 15(1)(h)); Right not to be subject to an ADM decision (Art. 22) and Right to human intervention (Art. 22(3)) » Accountability (Art. 5(2) & Art. 24(3)) » Data protection by design (Art. 25) » Processor due diligence (Art. 28(1)) » Security (Art. 32) » DPO (Art. 37 & 38)
Transparency	» Transparency (Art. 13 & 14) » ADM (Art. 22)
Diversity, Non-Discrimination and Fairness	» Fairness data protection principle (Art. 5.1(a)) » Risk assessment and DPIA (Art. 35) » Right to information on ADM and logic involved (Art. 15(1)(h))
Societal and Environmental Wellbeing	» Risk assessment and DPIA (Art. 35) » Transparency (Art. 13 & 14)
Accountability	» Accountability (Art. 5(2) & 24(3)) » Risk assessment and DPIA (Art. 35) » Processor due diligence (Art. 28(1)) » DPO (Art. 37 & 38)

CIPL AI and GDPR table[25]

4. Where do we want to go?

4.1 Future challenges and opportunities

In the Communication on Fostering a European approach to Artificial Intelligence, the European Commission wrote that, *"AI can significantly contribute to the objectives of the EU Security Union strategy. It can be a strategic tool to counter current threats and to anticipate both future risks – including hybrid threats – and opportunities. AI can help to fight crime and terrorism, and enable law enforcement to keep pace with the fast developing technologies used by criminals and their cross-border activities".* [26]

Especially in the fields of cybercrime and counterterrorism investigators face complex international networks, which require the analysis of huge amounts of data. These time sensitive operations could benefit enormously from the support of cutting-edge AI systems to understand and unveil the criminal structures behind the (potential) attacks. In addition, virtual reality can help visualising the findings and can be helpful in later criminal proceedings.

The Commission therefore embraces the opportunities of AI in the law enforcement sector, which is also reflected by projects like INFINITY. Nevertheless, these techniques could at the same time pose a threat to the rights and freedoms of individuals. The Proposal of the AI Regulation tries to find the balance between enabling the opportunities of AI systems and the same time protecting the fundamental rights and freedoms of people. The main challenges are namely the comprehensibility of decisions based on AI algorithms, (hidden) biases and difficulties correcting erroneous decisions.[27]

4.2 Outlook

This first proposal for a draft legislation by the Commission that was analysed above, is only one of the first steps in a likely multi-year process that will lead to a regulation coming into effect. To predict when exactly the AI Regulation will come into effect and what exact requirements will be applicable to developers and users of AI systems, would only be speculation. This is especially true for the Law Enforcement sector, since the outcome in this sensitive area will be, even more than other aspects, subject to protracted and emotionally charged political debates. In an exemplary manner, the European Parliament has already adopted several resolutions on AI.[28] The Committee on Civil Liberties, Justice and Home Affairs (LIBE) has just recently adopted a resolution on Artificial Intelligence in policing, and called, that the use of Artificial Intelligence in law enforcement and the judiciary should be subject to strong safeguards and human oversight. MEPs demand, among other things, a ban of private facial recognition databases, behavioural policing and citizen scoring.[29] Considering the European Parliament's role as co-legislator, this is further indication that these debates are about to follow and the outcome of the legislative process can hardly be anticipated.

References

Image Credits

Image from Gerd Altmann - https://pixabay.com/images/id-4791810/

Image from Pete Linforth - https://pixabay.com/illustrations/gdpr-security-data-protection-3438451/

Imge from Tumisu - https://pixabay.com/illustrations/gdpr-privacy-europe-eu-authority-3518254/

Image from kiquebg - https://pixabay.com/photos/technology-hands-agreement-okay-4256272/

1 EC, Proposal for a regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) COM/2021/206/final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (accessed 07.07.2021).

2 AI HLEG, Ethics Guidelines for Trustworthy AI https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines/1.html (accessed 08.07.2021).

3 EC, White Paper on Artificial Intelligence – A European approach to excellence and trust (Feb. 19, 2020), available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed 08.02.2020).

4 The results of the consultation process can be found here: https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence (accessed 06.02.2020).

5 EC, White Paper on Artificial Intelligence – A European approach to excellence and trust (Feb. 19, 2020), available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed 08.02.2020).

6 Press release: Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682 (accessed 12.06.2021).

7 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM(2021) 206 final.

8 Article 3(1) Proposal Artificial Intelligence Act, COM(2021) 206 final.

9 Press release: Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682 (accessed 12.06.2021).

10 Article 5(1) Proposal Artificial Intelligence Act, COM(2021) 206 final.

11 Article 5(1)(d) Proposal Artificial Intelligence Act, COM(2021) 206 final.

12 Press release: Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682 (accessed 12.06.2021).

13 As prominently invoked by the EC in its White Paper on AI regulation.

14 EDPB, Response to an MEPs letter on unfair algorithms, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out2020_0004_intveldalgorithms_en.pdf (accessed 17.02.2021).

15 GDPR, Article 22(2).

16 Directive 2016/680, Art. 11(1).

17 Directive 2016/680, Art. 11(3)

18 Article 29 Working Party, Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, WP251rev.01, As last Revised and Adopted on 6. February 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (accessed 23.11.2020).

19 FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement (2019) https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (accessed 22.11.2020).

20 EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (13 November 2019) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (accessed 12.02.2021).

21 CIPL, Artificial Intelligence and Data protection: How the GDPR regulates AI (2020) (available here: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_-1.pdf (accessed 01.02.2021) p. 13.

22 European Data Protection Supervisor, 'EDPS Opinion on the European commission's White Paper on Artificial Intelligence – A European approach to excellence and trust' (29 June 2020) https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf (accessed 19.02.2021) page 15.

23 Article 29 Data Protection Working Party, 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, (as last revised and adopted 4 October 2017) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

24 ICO, Guidance on DPIA https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when4

25 CIPL, Artificial Intelligence and Data protection: How the GDPR regulates AI (2020) (available here: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/03/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_-1.pdf (accessed 01.02.2021) p.18f.

26 Communication on Fostering a European approach to Artificial Intelligence; available at https://digital-strategy.ec.europa.eu/en/library/communication-fostering-european-approach-artificial-intelligence (accessed 04.08.2021).

27 Communication on Fostering a European approach to Artificial Intelligence, page 4.

28 E.g.: European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.pdf (accessed 01.01.2021).

29 LIBE, Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)) to be found here https://www.europarl.europa.eu/news/de/press-room/20210624IPR06917/artificial-intelligence-in-policing-safeguards-needed-against-mass-surveillance (accessed 08.07.2021).