Queen Mary, University of London
Mile End Road, London E1 4NS
Department of Law
Tel: + 44 (0)20 7882 3936
Fax: + 44 (0)20 7882 7042
www.law.qmul.ac.uk

University of Portsmouth
Portland Street, Portsmouth, PO1 3DE
Faculty of Business and Law
Tel: +44 (0)23 9284 6970
www.port.ac.uk

Doughty Street Chambers
54 Doughty Street, London, WC1N 2LS
Tel: +44 (0)20 7404 1313
Fax: +44 (0)20 7404 2284
www.doughtystreet.co.uk

CECLS:
Centre d'études sur les conflits
Tel: +33613061676
http://www.cecls.eu/fr/

Shaping Europe's Digital Future: A Response to The Commission's White Paper on Artificial Intelligence COM(2020)65 final, 19.2.2020

Jean Monnet Professor *ad personam* Elspeth Guild, Queen Mary University of London and Emeritus Professor of Law Radboud University Netherlands; Dr Elif Mendos Kuskonmaz, Lecturer in Law, University of Portsmouth; Dr Rowena Moffatt, Barrister, Doughty Street Chambers; Professor Didier Bigo, Director of Centre d'études sur les conflits and Professor of War Studies at King's College London and Research Professor at Sciences-Po, Paris

On 19 February 2020 the European Commission published its White Paper 'On Artificial Intelligence – A European approach to excellence and trust. This is a most timely contribution to the debate on the regulation of developing technologies and their commercial and state use. It is a pity that the White Paper has been issued before publication of the Commission's Advisory Committee on Equal Opportunities for Women and Men Opinion on Artificial Intelligence which is anticipated shortly. Similarly, both the EU Gender Equality Strategy is addressing the issue and a report will be published shortly on the same subject by the European Network of Equality Bodies (Equinet). Undoubtedly the White Paper would have been enhanced had it been informed also by the reports of these bodies which will appear shortly. This is particularly the case as the White Paper itself recognises that avoiding prohibited discrimination is one of the central challenges of AI deployment.[1]

In this response to the White Paper, we will address five issues:

1. The definition of AI and the centrality of access to data – the considerations which need to be taken into account;
2. The challenge of automated decision-making and Member State ratification of the Council of Europe's Convention 108+, ensuring coherence;
3. Data-sharing among public and private sector actors – coherence and consistency with the data protection principle of purpose limitation and consent of the data subject;
4. Remedies: how to regulate AI to ensure that decision-making is not obscured, including the material taken into account in ways which make the exercise of appeal rights and remedies inaccessible or impaired or nullified;
5. Trust and Oversight: ensuring that EU citizens have trust in AI uses through robust and effective oversight.

[1] See European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final, 19.02.2020, p. 11: "Bias and discrimination are inherent risks of any societal or economic activity. Human decision-making is not immune to mistakes and biases. However, the same bias when present in AI could have a much larger effect, affecting and discriminating many people without the social control mechanisms that govern human behaviour."

Defining AI and its relationship with data

As the White Paper recognises, there is a need to capture the concept of AI in a legally appreciable definition if it is to be regulated. The initial definition on page 2 "AI is a collection of technologies that combine data, algorithms and computing power" is unfortunately ambiguous. Most of the technical work on AI recognises the centrality of access to data. This includes personal data and data which can reveal the identities of the data subjects. Our concern here is that even at the outset of the White Paper there is a lack of clarity that the essence of AI uses depends on access to as large as possible sources of data, databases and similar venues where data is held. Much of this data will be personal data protected by the GDPR and Law Enforcement Directive. We will come back to this issue in the third section on the public-private intersection.

Two further definitions of AI are referred to in the White Paper – one from COM(2018) 237 final,[2] the other from the High Level Expert Group.[3] As the White Paper makes clear "without data, there is no AI" (p 19). While there is substantial concern expressed regarding 'high risk' uses of AI and how they should be defined and regulated, the question which precedes this one is: on what basis should AI algorithms have access to personal data stored in various public and private databases. The principle of the GDPR is that the consent of the data subject is necessary unless one of the enumerated exceptions apply (see below). The Regulation defines data as "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4(1)). Consent is defined as "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;" (Article 4(11)). Article 6 makes consent

[2] European Commission Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2018) 237 final, 25.04.2018, p. 1: "Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)."

[3] High Level Expert Group on Artificial Intelligence, 'A definition of AI: Main Capabilities and Disciplines', 8.04.2019, p. 8: "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions."

the default position for processing of personal data.[4] The requirement of consent (or even the application of one of the exceptions) is central to the foundation of data protection: personal data can only be processed for the purpose of which it was collected and in respect of which the data subject has given express consent. This is the principle of purpose limitation.

It is unclear from the White Paper exactly how the data subject's interest in the use of his or her data will be fully protected under the new approach, particularly in light of the purpose limitation on the use of data.

We consider this question to be fundamental to the whole thrust of the White Paper, to ensure that personal data is fully protected in a manner consistent with the GDPR (unamended), then the use of AI must be limited to data which either is not personal (nor can be identified back to the individual) or where the data subject has given explicit consent. The EU has spent substantial energy and time in designing the GDPR and adopting it. Member States and the private sector have invested heavily in ensuring that all their systems are compliant with the GDPR. We recognise that the GDPR and its underlying principles may hamper data-brokers regarding making a profit from the collection (including by web-scraping) and sale of personal data in the EU. It may also hamper technology companies from selling products based on the manipulation of vast quantities of personal data held in various public and private databases. But this is the ethical choice which the EU has made and incorporated into law. Indeed, the choice of protection of personal data was essential in the first data protection directive adopted in 1995 and strengthened in 2016 in full recognition of the changes and developments in technology. Judicial protection of personal data evidenced, *inter alia*, by the Court of Justice's 2014 decision in *Digital Rights Ireland*[5] was taken into account by the EU legislator in the adoption of the GDPR. This legislative, parliamentary and judicial consensus must be respected.

[4] "Processing shall be lawful only if and to the extent that at least one of the following applies:
(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."

[5] Grand Chamber, Digital Rights Ireland Ltd. (C–293/12) v. Minister for Communications, Marine and Natural Resources, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1.

The Challenge of Automated Decision Making

The White Paper recognises the problem of opacity ('black box effect') of many AI technologies (p 12). We will return to the consequences of this effect for remedies and judicial oversight below but here we wish to focus on the Council of Europe's new Convention 108+ and the regulation of new technologies in that venue. The EU Member States are in the process of ratifying this convention which updates its 1981 predecessor regarding the protection of individuals with regard to the processing of personal data. The obligation of data subject consent to use of his or her data is enshrined there (Article 5). Transparency of processing is covered in Articles 8 and 9 sets out the rights of the data subject. Further, Article 10 placed additional obligations on states to ensure that data controllers fully comply with the rules. The explanatory memorandum has been endorsed by the Committee of Ministers and forms part of the context in which the meaning of the terms is to be ascertained. It states that it is essential that an individual who may be subject to a purely automated decision has the right and power to challenge the decision. It expresses particular concern in respect of cases where individuals are stigmatised by application of algorithmic reasons. "Data subjects should be entitled to know the reasoning underlying the processing of data, including the consequences of such a reasoning which led to any resulting conclusions, in particular in cases involving the use of algorithms for automated decision-making including profiling." (Para 77)

Any EU measures which are proposed need to take into account the high threshold set out in Convention 108+ so that Member States are not placed in the position of having to regulate two different regimes where standards are lower in one when compared to the other. Convention 108+ is particularly explicit on the need in all cases for transparency, legal certainty, predictability and fairness of the processing of personal data. Individuals can only have remedies against automated decision making when these characteristics are present. We will return to this in the section on remedies and oversight, below. Suffice it here to suggest that in addition to a priori assessments of algorithms and data sets in the development phase, peer review, approval and licencing obligations are useful. There have been used in legislation in some countries such as Canada to safeguard standards.

Data sharing among public and private sector actors

The White Paper considers the application of AI among private sector as well as public sector actors with references to its use by law enforcement and judiciary (p. 10), but does not expressly mention any data-sharing activities between two sectors to implement the data later in AI technologies. The European Commission's Communication on the European data strategy that was published on the same day as the White Paper, however, refers to a cross-sectoral governance framework for data access and use (p. 12).[6] We consider that the EU needs to proceed with great caution in respect of this initiative.

[6] European Commission 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, COM(2020) 66 final, 19.2.2020.

As the White Paper recognises, advances in digital technology and its ever-evolving integration into everyday aspects of our lives have resulted in collecting and analysing great amounts of data more efficiently.[7] Most of this data however has been collected by private sector actors for their own business purposes and in relation to individuals' online activities as customers of their services. Because the private sectors' needs regarding data accuracy are frequently not particularly rigorous, for instance errors in names and telephone numbers may not be particularly important but credit card details are, the use of this personal data for other purposes may have the effect of multiplying inaccuracies. The common presumption is that the more input data that AI tools have, the better they become at performing their tasks. We are concerned that equipping public sector actors with AI tools would lead to introducing requirements on private sector actors to release to state authorities extensive personal information that they hold on their customers.

Any such plan represents a challenge to the data protection principle of purpose limitation, fair and lawful processing. Data subject's consent is one of six lawful grounds for data processing under the GDPR, however, when the private sector ties data subject's consent into their contracts or provisions of services, issues arise whether that consent is 'freely' given. The former Article 29 Working Party explicitly recognised during its assessment on consent under the GDPR that individuals do not give free consent to non-negotiable part of contracts.[8] The Court of Justice also considered that if the data subject has no real choice of objecting the processing of personal data, consent could not be considered freely given.[9] Even if consent may not be undermined because of how private sector obtains it from its customers, releasing personal data to state authorities would be contrary to purpose limitation, according to which data must be collected for specified and legitimate purposes and cannot be used for another purpose that is incompatible with the original purpose.

We also consider that any potential private-public collaboration on AI tools needs to identify clearly the applicable EU legal framework on data protection. The GDPR sets forth general data protection principles applicable to all sectors when they process personal data, but it excludes processing of personal data for the purposes of preventing, investigating, detecting and prosecuting criminal offences (Art 2(2)). The Law Enforcement Directive covers processing of personal data in this specific area on the condition that it is carried out by

[7] European Commission, 'White Paper' (n 1), p. 4: "The volume of data produced in the world is growing rapidly, from 33 zettabytes in 2018 to an expected 175 zettabytes in 2025. Each new wave of data brings opportunities for Europe to position itself in the data-agile economy and to become a world leader in this area. Furthermore, the way in which data are stored and processed will change dramatically over the coming five years. Today 80% of data processing and analysis that takes place in the cloud occurs in data centres and centralised computing facilities, and 20% in smart connected objects, such as cars, home appliances or manufacturing robots, and in computing facilities close to the user ("edge computing"). By 2025 these proportions are set to change markedly."

[8] Working Party, Guidelines on Consent under Regulation 2016/679 (28.11.2017) https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

[9] Fourth Chamber, Michael Schwarz (C-291/12) v. Stadt Bochum, http://curia.europa.eu/juris/liste.jsf?num=C-291/12.

'competent authority'.[10] The Directive might cover a private sector actor if it is 'entrusted by a Member State's law to exercise public authority and public powers' to process personal data for the purposes of preventing, investigating, detecting and prosecuting criminal offences. Unless otherwise 'entrusted' by law, the GDPR applies to that type of processing by private sector actors. Even if it is 'entrusted' to process personal data for law enforcement related purposes, the applicability of the GDPR and Law Enforcement Directive depends on the purpose of *transfer*. If the transfer from competent authority to non-competent authority takes place for law enforcement purposes, the Directive applies to that processing. If the transfer from a competent authority to another competent authority takes place for non-law enforcement related purposes, the GDPR applies.

We would highlight that this shift in establishing the applicable legislative framework is important because of different levels of protection afforded under the GDPR and the Law Enforcement Directive. The Directive as the chosen legal act in the field of law enforcement related purposes provides a certain leeway to Member States to implement data protection principles contained therein 'as far as possible.'[11] We understand that this might be necessary to address the special needs of data processing for law enforcement purposes and diverse laws among Member States, however, it must be recognised that how the Directive is transposed at national level bears particular importance for privacy and data protection against AI tools. The Charter provides the minimum fundamental rights standard and it must be respected in the application of the Directive. Finally, there are a number of *lex specialis* laws that govern the processing of personal data in the Area of Freedom, Security and Justice (AFSJ) and we are concerned with the level of protection that they afford if and when AI tools are used in areas they cover.[12]

Remedies

We are in full agreement with the view taken in the White Paper that AI, if unregulated or regulated ineffectively, may lead to the breach of fundamental rights, including the rights to an effective legal remedy and a fair trial, as protected within the EU by Article 47 of the Charter, Article 6 ECHR and the general principles of EU law. The particular challenges involved in ensuring access to a remedy and procedural fairness from automated decision-making ('ADM') relate to transparency, unpredictability and complexity, which are anathema

[10] 'Any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security; or any other body or entity entrusted by Member State law to exercise public authority and public powers for these purposes.' Law Enforcement Directive art 3(7)(a).

[11] Law Enforcement Directive art 5.

[12] Examples include 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 [2018] OJ L 295; Directive 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L119/132; Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2006] OJ L381/4.

to the rule of law (and the principles recognised in the new Convention 108+, as we set out above). As noted in the White Paper, the challenging characteristics of AI technologies (including opacity, complexity and unpredictability) may hamper the efforts both of enforcement agencies and individuals to hold decision-makers and other entities to account. In particular, an individual may be unable to know whether a decision affecting him or her has been taken wholly or in part by AI; may be unable to know or understand the reasons for that decision; and may not have access to an effective legal route in order to bring a challenge. There are, therefore, urgent and grave risks to the rule of law posed by AI. In a worst case scenario, the subjects of adverse decisions would be placed in a 'Kafkaesque' situation whereby they would be prevented from knowing the criteria against which an adverse decision was taken or the reasons for which they were unsuccessful.

Whilst we acknowledge the national procedural autonomy of Member States, a failure to provide protection for the rule of law at an EU-level from the risks posed by AI would be damaging both to the internal market and to the European legal values as enshrined in the Charter on Fundamental Rights. We note the efforts of other States to regulate ADM and ensure access to justice from automated systems.[13] Taking into account the risks posed by ADM as set out above and in the White Paper, we are of the view that the minimum requirements to protect access to effective legal remedies and the rule of law within the EU should include:

(i) a requirement of advance notice that ADM systems will be used to be given to all those affected by its decisions;

(ii) a requirement that full reasons and explanations of how and why a decision was made be given with the notification of outcome; and

(iii) avenues of independent and impartial judicial recourse from ADM.

We also question whether at this stage of software development and in the absence of clear assurances as to the quality of data and information input in ADM, a fully automated decision (as opposed to assisted digital decision-making, where a human retains ultimate decisional control) would be compatible with the requirements of procedural fairness. Indeed, it would appear to us that certain decisions cannot fairly be taken fully by AI at current stages of development (if at all) and certainly clear that it would be inappropriate where human rights were at stake. In this context, it would be useful for the White Paper to distinguish – in the context of procedural justice – between fully automated decision-making and automation by way of decisional support in which discretion is retained by a human.

Moreover, we note that procedural requirements as to notice, the duty to give reasons, and the existence of judicial avenues of redress may prove ineffective unless the data and information used by ADM is free from unintended biases and other problems that may unfairly affect outcomes. For this reason, we recognise that there is need for transparency, testing and monitoring of both data and ADM software prior to permission being granted for its use in decision-making. As such, there needs to be a robust system for validating the quality

[13] See, eg, Canadian Directive on Automated Decision-Making: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.

and reliability of both the data and information used in ADM and the ADM software. We are of the view that the use of ADM by public authorities for any type of decision-making should be subject to the same public law requirements as for any other proposed project. This would include public consultation phases, requirements of transparency as to data inputs and the mechanics of decision-making, and notice requirements.

Trust and Oversight

The tone of the White Paper is deliberately enthusiastic about progress in this field and optimistic about the benefits of big data and AI. While good reasons may exist for this position in general terms, the elephant in the room is undisclosed surveillance, by both public and private sectors. Public and consumer trust in AI and data analytics is only possible if the context of covert surveillance is taken into account as well as the use of AI in internal security matters (as opposed to defence). At least two separate problems need to be taken into account: first the opacity legitimated in directives and legislation on trade secrets, secondly the diverse legislation concerning interception of data by Sigint (Signals Intelligence) and other agencies in their tasks of surveillance, outside of the context of war, but nevertheless justified on the basis of national security arguments. These state agencies are thereby authorised to use black boxing software and AI technologies but with little or no accountability. In light of these two issues we make the following comments.

First: the objective of the strategy is to reinforce trust by citizens in AI. This is a key element. Yet, the origins of the lack of trust are never set out. The text refers to a general unease with AI and robots but does not address the crisis of confidence which followed the Snowden disclosures in 2013 about the US-led Five Eyes surveillance practices and in particular the NSA GCHQ practices of snooping on EU citizen and their institutions. Thus, only part of the picture is presented in the strategy. The emphasis on human oversight of the uses of AI is certainly present in the text and very well discussed in general terms. It is clear that for small and middle size companies working in Europe or seeking to enter the European market a new series of assessments regarding their AI use including algorithms will be mandatory. But this does not address the source of EU citizens' distrust of AI and the use of their data. Only on page 18 point 4 does the Paper quote an excerpt from the Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics signalling the current opacity of algorithms in AI systems and the "necessity of transparency requirements". This declaration is not sufficient. On a more positive note, the strategy under the part on compliance and enforcement declares that "an objective, prior conformity assessment would be necessary to verify and ensure that certain of the above-mentioned mandatory requirements applicable to high-risk applications (see section D above) are complied with. The prior conformity assessment could include procedures for testing, inspection or certification. It could include checks of the algorithms and of the data sets used in the development phase." Leaving aside the issue of the tentative language, used (we would make the a priori testing mandatory) and its limitation to high-risk applications rather than all applications which engage personal data, there are important lacunae. One of the most important problems concerning citizens' trust of companies collecting or selling their data is not addressed i.e. the claimed right of companies to keep secret the commercial

mathematical formulae of their algorithms from any authorities. It is this lack of accessibility that creates the possibility to develop black boxing designs and-or machine learning discriminating effect which are often dependent of biases coming from the difference between the sample population and the final one. In order for a priori or ex post oversight mechanisms to be effective there has to be a clear and unconditional limitation on the 'trade secrets' exception. Companies must not have the possibility to hide their developments behind the cloak of intellectual property protection. The Commission must be ready to challenge this restriction both in respect of public agencies and the private sector, in particular those parts which work in the security and intelligence sectors.

An effective oversight mechanism means that an independent agency needs to have access to the proprietary algorithms to run tests on their purposes and on their unintentional side effects in terms of statistical discrimination or use to target suspicious behaviours. It is not certain that the White Paper's proposed conformity assessment procedures on the development phase will be a sufficiently robust test if the agency in carrying out the assessment does not have access to the final programme. Oversight, necessity and proportionality of AI mechanisms depends on full and unfettered access to these elements. As long as black boxing is a common practice protected by intellectual property rules, it will be impossible to speak of a trustworthy system with a fair competition in the field of AI.

Any new powers for an agency to carry out assessments must clearly deal with the national transposition of Directive 2016/943 (8 June 2016) on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure which is currently being used by large technology companies to block exactly this kind of accountability.

Already, the EDPS has proposed that it should be mandated to carry out oversight of the use of big data and AI. This is a good suggestion, but the budget and personnel of the EDPS must be increased proportionately if it is to be given this new power. The resources at the command of the large technology companies and the degree of resistance to transparency by both public and private sectors engaged in the security sector mean that the EDPS (or a new agency) will need very substantial financial and other support if it is to carry out this job satisfactorily. In light of past failures which have weakened public trust in AI and use of personal data, to re-establish trust, this agency and its effective operation is crucial.

Second: If the Commission's text is oriented towards the predictive use of AI, it is worth acknowledging that this is a key source of EU citizens' mistrust of what is known as dataveillance. Reference to mass surveillance by state authorities is only made once on page 11. On reading the White Paper one would think that the Snowden disclosure of the NSA practices never happened. Further, much legislation adopted after 2013 and presented as 'resolving' the dataveillance issue have merely justified the use of data interception at a large scale size and the running of specific algorithms based on big data and AI. The White Paper does not recognise this as such instead only referring vaguely to law enforcement authorities' policing, crime and criminal justice systems. Unfortunately the lack of confidence of internet users in digital activities and profiling does not come from criminal justice policing but from

preventive predictive intelligence. Data-sharing practices where the data of European citizens are considered as an easy prey, which can be used and trade later on for policing purposes and commercial ones (such as facial recognition, the only issue raised as of serious concern in the White Paper in this area) is a prime source of mistrust among Europeans. Any EU strategy for a digital future has to respond to this challenge of interception of personal data and its sharing beyond purpose limitation, carried out by intelligence services (outside the context of military interventions abroad), and Sigint collaboration. This is also the case for more mundane transatlantic collaboration on the surveillance on border flows (of goods, people, money) by police, border guards and/or customs officials, often via forms of data exchange and-or interoperability of databases and open selectors, which are not properly accountable. If the use of AI algorithms of surveillance by Sigint, both police and intelligence, is not addressed, it may destroy any chance of regaining the trust of EU citizens.

Conclusions

While we welcome the Commission's White Paper, we consider that further clarifications would be helpful. We have five main proposals:

1. The definition of AI needs to be clear and precise and it dependence on data (including personal data) acknowledged from the outset;
2. The EU standards of protection of individuals in the face of AI uses must be at least as high if not higher than those contained in the Council of Europe's Convention 108+ currently being ratified by the Member States;
3. Data sharing among public and private sector actors must fully comply with both the GDPR (where applicable) and the Law Enforcement Directive (where relevant). The principle of data subject consent and purpose limitation must be fully respected in the use of both public and private sector data;
4. It is crucial that individuals affected by ADM have remedies and avenues to challenge outcomes. This is particularly urgent in light of the capacity of AI to profile on prohibited grounds of discrimination;
5. The trust of EU citizens in AI applications must be earned. This is particularly important in light of the abuses of EU citizens' privacy which revelations about mass, covert surveillance by public and private agencies have shown. EU citizens are entitled to robust and effective oversight of all AI uses both public and private. That oversight must include a priori and continuous assessment of algorithms and data sets, peer review, approval and licencing as regulatory mechanisms to ensure that EU citizens can trust AI processes.