The Information Commissioner's response to the Council of Europe, Ad hoc Committee on Artificial Intelligence (CAHAI) multi-stakeholder consultation

Contents

About the ICO 1
Introduction 1
Consultation response 2
Section 1: Definition of AI Systems 2
Section 2.1: Opportunities and Risks arising from AI Systems 3
Section 2.2: Impact on human rights, democracy and the rule of law 5
Section 3: Potential Gaps in Existing Binding Legal Instruments Applicable to AI 9
Section 4: Elements of a Legal Framework on AI Systems 11
Section 5: Policies and Measures for Development 13

About the ICO

The Information Commissioner has responsibility in the UK for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003 (PECR), amongst others.

The Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations and taking appropriate action where the law is broken.

Introduction

The Information Commissioner's Office (ICO) welcomes this opportunity to respond to the CAHAI multi-stakeholder consultation on behalf of the Commissioner. Enabling good practice in AI[1] is a priority for the ICO.

[1] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/new-priorities-for-uk-data-protection-during-covid-19-and-beyond/

Amongst other things, we do this by publishing guidance on our website, supporting organisations in our Regulatory Sandbox, and playing an active role in national and international AI policy discussions, offering our expertise on data protection (DP) and the right to privacy. We reference this work in our response below, and provide links to relevant resources were possible.

We note that the multi-stakeholder consultation, and the work of the CAHAI, touches on a broad range of issues relevant to AI. We have limited our response to areas within the limits of our regulatory remit and / or where we have developed policy positions. This means that for some questions we respond as 'no opinion'. Where appropriate, we also provide additional detail that explains our responses to the multiple-choice questions. This is found in our response to question 40 - the final question of the consultation.

Consultation response

[Questions 1 to 6 relate to pre-screening information]

Section 1: Definition of AI Systems

7. In view of the elaboration of a legal framework on the design, development and application of AI, based on the standards of the Council of Europe on human rights, democracy and the rule of law, what kind of definition of artificial intelligence (AI) should be considered by the CAHAI

- ❑ No definition, with a legal instrument focused on the effect of AI systems on human rights, democracy and the rule of law
- ☒ A technologically-neutral and simplified definition, such as "a set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being" (See the CAHAI feasibility study, §5)
- ❑ A definition focusing on machine learning systems
- ❑ A definition focusing on automated decision-making
- ❑ Other
- ❑ No opinion

8. What are the reasons for your preference?

We welcome the Feasibility Study's conclusion that a consensus appeared to arise on the need "to approach AI systems in a technologically neutral way, comprising all the various automated decision-making technologies that fall under this umbrella term, including their broader socio-technical context".

Given the speed of AI development it is important for regulatory frameworks to avoid being too specific or risk becoming obsolete as the technology evolves. We believe a practical definition of Artificial Intelligence that covers a wider range of technologies rather than a more prescriptive one will be able to remain current as the technology progresses. A definition focusing on machine learning systems for instance, could leave a substantial portion of applications out of scope.

Section 2.1: Opportunities and Risks arising from AI Systems

9. Please select the areas in which AI systems offer the most promising opportunities for the protection of human rights, democracy and the rule of law

- ❑ Banking, finance and insurance
- ❑ Justice
- ❑ Law enforcement
- ❑ Customs and border control
- ❑ Welfare
- ❑ Education
- ❑ Healthcare
- ❑ Environment and climate
- ❑ Election monitoring
- ❑ National security and counter-terrorism
- ❑ Public administration
- ❑ Employment
- ❑ Social networks/media, internet intermediaries
- ❑ Other
- ☒ No opinion

10. If other, which areas and why?

We agree with the Feasibility Study's suggestion that a risk-based approach should target "the specific application context". AI can be applied in various different contexts in each of the domains listed here. Therefore it is difficult for the ICO to put forward a broad statement in relation to each of those domains without taking into account the specific context and the problem the deployment of AI seeks to tackle.

As part of its Regulatory Sandbox service, the ICO has worked with a number of organisations across different sectors that are using AI to deliver promising products whilst ensuring people's privacy and data rights are

protected. Furthermore, we are launching an AI Risk Toolkit which will supplement our guidance on AI and data protection, and provide risk practitioners with practical support in assessing AI systems' risk. We believe a practical orientated approach to assessing risk and harm supports developers of AI systems in ensuring human rights and freedoms are protected and respected throughout the lifecycle of AI development and use.

11. Please indicate which of the following AI system applications in your view have the greatest potential to enhance/protect human rights, democracy and the rule of law?

- ❑ Facial recognition supporting law enforcement
- ❑ Emotional analysis in the workplace to measure employees' level of engagement
- ❑ Smart personal assistants (connected devices)
- ❑ Scoring of individuals by public and private entities
- ❑ Medical applications for faster and more accurate diagnoses
- ❑ Automated fraud detection (banking, insurance)
- ❑ AI applications to predict the possible evolution of climate change and/or natural disasters
- ❑ AI applications for personalised media content (recommender systems)
- ❑ Deep fakes and cheap fakes
- ❑ Recruiting software/ AI applications used for assessing work performance
- ❑ AI applications to prevent the commission of a criminal offence (e.g. anti-money laundry AI applications)
- ❑ AI applications aimed at predicting recidivism
- ❑ AI applications providing support to the healthcare system (triage, treatment delivery)
- ❑ AI applications determining the allocation of educational services
- ❑ AI applications determining the allocation of social services
- ❑ AI applications in the field of banking and insurance
- ☒ AI applications to promote gender equality (e.g. analytical tools)
- ❑ AI applications used for analysing the performance of pupils/students in educational institutions such as schools and universities

12. Please briefly explain how such applications would benefit human rights, democracy and the rule of law

Even though various applications mentioned above could benefit human rights, democracy and the rule of law, we felt AI applications promoting gender equality fall closer to our remit, in the context of data protection's

fairness principle. Bias and discrimination is an issue of increasing importance in the AI space and one the ICO is engaging with.

In general, we agree with the Feasibility Study in that "the positive or negative consequences of AI systems depend also on the values and behaviour of the human beings that develop and deploy them", so it is important to focus on human responsibility as much as the computational/machine processes themselves.

13. What other applications might contribute significantly to strengthening human rights, democracy and the rule of law?

We believe applications that foster citizen engagement and support digital, data and AI literacy could contribute towards those goals.

Section 2.2: Impact on human rights, democracy and the rule of law

14. Please select the areas in which the deployment of AI systems poses the highest risk of violating human rights, democracy and the rule of law

- ❑ Banking, finance and insurance
- ❑ Justice
- ❑ Law enforcement
- ❑ Customs and border control
- ❑ Welfare
- ❑ Education
- ❑ Healthcare
- ❑ Environment and climate
- ❑ Election monitoring
- ❑ National security and counter-terrorism
- ❑ Public administration
- ❑ Employment
- ❑ Social networks/media, internet intermediaries
- ☒ No opinion

15. Please briefly explain how such applications might violate human rights, democracy and the rule of law

Mirroring our response to question 10, we believe AI applications can pose risks or create benefits in these sectors, depending on the specific context, the stated goal of the deployment and the governance structures that

surround it. Given the multitude of possible contexts within each of these domains, it is difficult to give a definitive answer to this question.

Nevertheless, it is worth noting that the ICO's guidance on AI and Data Protection explains how AI systems can lead to discrimination and impact individuals' right to privacy. Furthermore, we believe that infringements to rights are exacerbated where there is a lack of transparency and accountability for the affected citizen. Our guidance on explainability of AI, co-developed with The Alan Turing Institute, sets out the types of explanations that help improve transparency.

16. Please indicate the types of AI systems that represent the greatest risk to human rights, democracy and the rule of law

- ❑ Facial recognition supporting law enforcement
- ❑ Emotional analysis in the workplace to measure employees' level of engagement
- ❑ Smart personal assistants (connected devices)
- ☒ Scoring / scoring of individuals by public entities
- ❑ Medical applications for faster and more accurate diagnoses
- ❑ Automated fraud detection (banking, insurance)
- ❑ AI applications to predict the possible evolution of climate change and/or natural disasters;
- ❑ AI applications for personalised media content (recommender systems)
- ❑ Deep fakes and cheap fakes
- ❑ Recruiting software/ AI applications used for assessing work performance
- ❑ AI applications to prevent the commission of a criminal offence
- ❑ AI applications aimed at predicting recidivism
- ❑ AI applications providing support to the healthcare system (triage, treatment delivery)
- ❑ AI applications determining the allocation of educational services
- ❑ AI applications determining the allocation of social services
- ❑ AI applications in the field of banking and insurance
- ❑ AI applications to promote gender equality (e.g. analytical tools)
- ❑ AI applications used for analysing the performance of pupils/students in educational institutions such as schools and universities

17. Please briefly explain how such applications might violate human rights, democracy and the rule of law

Mirroring our response to question 12, we believe AI applications can pose risks or create benefits in these sectors. The governance and accountability structures, the context and the goal of the deployment, rather than just the technology itself will determine the level and nature of risk. With that in mind, applications that were not selected in question 16 may present risks but without additional contextual information it is not possible to estimate their risks. On the other hand, there is a growing consensus around the risks of public entities engaging in social scoring.

It is worth noting that the ICO has recently published the draft version of a data protection risk toolkit in the context of AI development and deployment. We will be further developing this toolkit and aim to release a beta version later this year after consulting with stakeholders. Separately, we have noted that most AI deployments will need a Data Protection Impact Assessment (DPIA) to identify, record and mitigate risks and adverse effects on individuals. Article 35(3) of the UK GDPR sets out three types of processing that trigger the need to conduct an DPIA: the systematic and extensive profiling with significant effects, large scare use of sensitive data and public monitoring. At least one of these processes takes place in many AI systems.

18. What other applications might represent a significant risk to human rights, democracy and the rule of law?

No opinion.

19. In your opinion, should the development, deployment and use of AI systems that have been proven to violate human rights or undermine democracy or the rule of law be

☒ Banned
❑ Not banned
❑ No opinion

20. In your opinion, should the development, deployment and use of AI systems that pose high risks* with high probability to human rights, democracy and the rule of law be**

*** High negative impact on human rights, democracy and rule of law**
**** High probability of occurrence of these risks**

❑ Banned
❑ Subject to moratorium
☒ Regulated (binding law)

❑ Self-regulated (ethics guidelines, voluntary certification)
❑ None of the above
❑ No opinion

21. In your opinion, should the development, deployment and use of AI systems that pose low risks* with high probability to human rights, democracy and the rule of law be**

*** Low negative impact on human rights, democracy and rule of law**
**** High probability of occurrence of these risks**

❑ Banned
❑ Subject to moratorium
☒ Regulated (binding law)
❑ Self-regulated (ethics guidelines, voluntary certification)
❑ None of the above
❑ No opinion

22. In your opinion, should the development, deployment and use of AI systems that pose high risks* with low probability to human rights, democracy and the rule of law be**

*** High negative impact on human rights, democracy and rule of law**
**** Low probability of occurrence of these risks**

❑ Banned
❑ Subject to moratorium
☒ Regulated (binding law)
❑ Self-regulated (ethics guidelines, voluntary certification)
❑ None of the above
❑ No opinion

23. What are the most important legal principles, rights and interests that need to be addressed and therefore justify regulating the development, deployment and use of AI systems?

Select 5 maximum

❑ Respect for human dignity
❑ Political pluralism
❑ Equality
❑ Social security

❑ Freedom of expression, assembly and association
☒ Non-discrimination
☒ Privacy and data protection
❑ Personal integrity
❑ Legal certainty
☒ Transparency
☒ Explainability
☒ Possibility to challenge a decision made by an AI system and access to an effective remedy

24. In your opinion, in what sectors/areas is a binding legal instrument needed to protect human rights, democracy and the rule of law?

Select 3 maximum

❑ Banking, finance and insurance
❑ Justice
❑ Law enforcement
❑ Customs and border control
❑ Welfare
❑ Education
❑ Healthcare
❑ Social networks/media, internet intermediaries
❑ Environment and climate
❑ Election monitoring
❑ Public administration
☒ No opinion

Section 3: Potential Gaps in Existing Binding Legal Instruments Applicable to AI

In the following section, please indicate to what extent you agree or disagree with the following statements or if you have no opinion on a given issue.

1=I completely disagree;
2=I rather disagree;
3=Indifferent/no opinion;
4=I rather agree;
5=I fully agree;

25. Self-regulation by companies is more efficient than government regulation to prevent and mitigate the risk of violations of human rights, democracy and the rule of law

Rating: 2

26. Self-regulation by companies is sufficient to prevent and mitigate the risk of violations of human rights, democracy and the rule of law

Rating: 2

27. Which of the following instruments of self-regulation do you consider to be the most efficient?

Single choice.

❑ Ethics guidelines
❑ Voluntary certification
☒ No opinion

28. Existing international, regional and/or national binding and/or non-binding legal instruments are sufficient to regulate AI systems in order to ensure the protection of human rights, democracy and the rule of law

Rating: 2

29. If you responded disagree/completely disagree to previous question, please indicate why existing international, regional and/or national (binding and/or non-binding) legal instruments are not sufficient to regulate AI systems

Select all you agree with

❑ There are too many and they are difficult to interpret and apply in the context of AI
❑ They provide a basis but fail to provide an effective substantive protection of human rights, democracy and the rule of law against the risks posed by AI systems
☒ They lack specific principles for the design, development and application of AI systems

☒ They do not provide enough guidance to the designers, developers and deployers of AI systems

❑ They do not provide for specific rights (e.g. transparency requirements, redress mechanisms) for persons affected by AI

❑ They create barriers to the design, development and application of AI systems

30. Please provide examples of existing international, regional and/or national (binding and/or non-binding) instruments that in your view are effective in guiding and regulating the design, development and use of AI systems to ensure compatibility with the standards for human rights, democracy and the rule of law

The ICO believes current binding instruments such as Convention 108, GDPR or in the UK the DPA 2018[2] can address the DP risks posed by AI systems but there may be other risks to other human rights mentioned in this questionnaire that will profit from a more comprehensive legal framework and enhanced cooperation to regulate the technology.

The ICO along with the FCA (the financial services regulator), the CMA (the competition regulator) and Ofcom (the communications regulator), have created the Digital Regulation Cooperation Forum (DRCF),[3] in the context of which we are collaborating to assess and address AI harms by building common capacity and sharing knowledge.

31. Please indicate other specific legal gaps that in your view need to be addressed at the level of the Council of Europe

No opinion

Section 4: Elements of a Legal Framework on AI Systems

In relation to some AI systems, we can reasonably foresee a significant risk to human rights, democracy and the rule of law. Bearing this in mind, in the following section, please indicate to what extent you agree or disagree with the following statements or if you have no opinion on a given issue.

32. Please indicate to what extent you agree or disagree with the following statements or if you have no opinion on a given issue

[2] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
[3] https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122

Required to answer. Likert.

I completely disagree;
I rather disagree;
Indifferent/no opinion;
I rather agree;
I fully agree;

- **Individuals should always be informed when they interact with an AI system in any circumstances:** No opinion

- **Individuals should always be informed when a decision which affects them personally is made by an AI system:** I rather agree

- **Individuals should always be informed when an AI system is used in a decision-making process which affects them personally:** No opinion

- **Individuals should have a right to a meaningful explanation of algorithmic based decisions, in particular how the algorithm reached its output:** I rather agree

- **Individuals should always have the right that any decision taken by an AI system in the framework of judicial proceedings are reviewed by a "human" judge:** I fully agree

- **Individuals should have a right to demand the review of an algorithmic based decision by a human being:** I rather agree

- **There should always be a person responsible for reviewing algorithmic based decisions in the public sector and private companies:** I rather agree

- **Public institutions should not use AI systems to promote or discredit a particular way of life or opinion (e.g. "social scoring"):** I rather agree

- **States should be obliged to design, develop and apply sustainable AI systems that respect applicable environmental protection standards:** No opinion

- **The code behind AI systems used in the public and private sectors should always be accessible to the competent public authorities for the purposes of external audit:** I fully agree

- **There should be higher transparency standards for public entities using AI than for private entities:** I rather agree

- **There should be higher standards for access to an effective remedy for individuals in relation to decisions informed and made by an AI system in the field of justice than in the field of consumer protection:** No opinion

- **Member States should establish public oversight mechanisms for AI systems that may breach legally binding norms in the sphere of human rights, democracy and the rule of law:** I rather agree

- **Errors and flaws discovered in AI systems which have led or could lead to the violation of human rights, democracy and the rule of law must be reported to the competent authorities:** I fully agree

- **The use of facial recognition in public spaces should be prohibited:** No opinion

- **The information obtained through the use of facial recognition systems should always be reviewed by a human being before being used for purposes that have an impact on individual freedom, such as in relation to a person boarding an airplane, upon police arrest or in the framework of judicial proceedings:** No opinion

- **The use of AI systems in democratic processes (e.g. elections) should be strictly regulated:** I fully agree

33. Should a future legal framework at Council of Europe level include a specific liability regime in relation to AI applications?

Single choice.

❑ Yes
❑ No
☒ No opinion

Section 5: Policies and Measures for Development

34. In your opinion, how useful would the following compliance mechanisms be in preventing and mitigating the risks to human rights, democracy and the rule of law arising from the design, development and application of AI?
Required to answer. Likert.

*** Intersectional audits consider intersection of multiple sensitive attributes (race, gender, etc) jointly instead of attributes alone - for an example of such audits with machine learning, see for instance: Morina, Giulio & Oliinyk, Viktoriia & Waton, Julian & Marusic, Ines & Georgatzis, Konstantinos. (2019). Auditing and Achieving Intersectional Fairness in Classification Problems**

Not useful;
Rather not useful;
Indifferent/no opinion;
Rather useful;
Highly useful;

- **Human rights, democracy and rule of law impact assessments:** Highly useful
- **Certification and quality labelling:** Highly useful
- **Audits and intersectional audits*:** Highly useful
- **Regulatory sandboxes:** Highly useful
- **Continuous automated monitoring:** Rather useful

35. Please indicate what combination of mechanisms should be preferred to efficiently protect human rights, democracy and the rule of law

Select 3 maximum

☒ Human rights, democracy and rule of law impact assessments
❑ Certification and quality labelling
☒ Audits and intersectional audits
☒ Regulatory sandboxes
❑ Continuous automated monitoring

36. Please select which mechanism(s) should be part of either a binding instrument or a non-binding instrument to best protect human rights, democracy and the rule of law

Required to answer. Likert.

Binding instrument;
Non-binding instrument;
No opinion

- **Human rights, democracy and rule of law impact assessments:** Binding instrument
  Certification and quality labelling: Non-binding instrument
- **Audits and intersectional audits*:** Binding instrument
- **Regulatory sandboxes:** Non-binding instrument
- **Continuous automated: monitoring** No opinion

37. If any other mechanism(s) should be considered, please list them and mention if they should be part of either a binding or non binding instrument

No opinion

38. In your opinion, how useful would the following follow-up activities be if implemented by the Council of Europe?

Likert.

Not useful;
Rather not useful;
Indifferent/no opinion;
Rather useful;
Highly useful;

- **Monitoring of AI legislation and policies in member States:** Highly useful
- **Capacity building on Council of Europe instruments, including assistance to facilitate ratification and implementation of relevant Council of Europe instruments:** Highly useful
- **AI Observatory for sharing good practices and exchanging information on legal, policy and technological developments related to AI systems:** Highly useful
- **Establishing a centre of expertise on AI and human rights:** Highly useful

39. What other mechanisms, if any, should be considered?

No opinion

40. Are there any other issues with respect to the design, development and application of AI systems in the context of human rights, democracy and the rule of law that you wish to bring to the attention of the CAHAI?

The ICO welcomes the opportunity to offer our views on this consultation as it has been active in AI policy discussions, offering its expertise on data protection (DP) and the right to privacy.

DP lies at the heart of the AI regulation debate and some of the principles and rights in point 23 of this questionnaire are at the centre of DP law. Transparency, explainability, non-discrimination and the ability to challenge a decision made by an automated decision-making system (ADMS) are supported by the UK GDPR, UK's Data Protection Act 2018 and the Convention 108.

We welcome the CAHAI's mapping of ethical AI guidelines that identified justice, privacy and fairness as the principles with most cross-geographical and cross-cultural congruence. Privacy and DP are fundamental rights protected under GDPR while fairness is one of its key principles. The commonalities in the debate over AI and DP regulation indicate data protection authorities, such as the ICO, have a vital role to play in the AI space by providing guidance, sharing best practice and testing new technologies in safe environments. We believe any new framework should not confuse or dilute DP law, and its existing principles, concepts and tools (eg DPIAs) can be enhanced or augmented (eg with a human rights impact assessment) but should not be replaced or duplicated.

The ICO was one of the first organisations to launch a Regulatory Sandbox[4] to test new technologies for DP compliance and is already building capacity in AI system auditing. Onfido[5] and Novartis[6] were some of the first companies building AI-driven products to go through the ICO's Sandbox.

The ICO has published guidance on Explaining Decisions Made with AI[7] (ExplAIn) and AI and Data Protection.[8] Our guidance states that most AI

[4] https://ico.org.uk/for-organisations/regulatory-sandbox/the-guide-to-the-sandbox/
[5] https://ico.org.uk/media/for-organisations/documents/2618551/onfido-sandbox-report.pdf
[6] https://ico.org.uk/media/for-organisations/documents/2619244/novartis-sandbox-report.pdf
[7] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-ai/
[8] https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-ai-and-data-protection

systems will require a Data Protection Impact Assessment[9] (DPIA) and the ICO has provided more detailed explanation of what that should entail Adaptive AI systems may require regular DPIAs to avoid the adverse impacts of any concept drift.

We have recently released the draft version of our AI and Data Protection Risk Mitigation and Management Toolkit and we are enhancing our capacity to audit AI systems for data protection compliance. We believe supporting those developing and deploying AI systems in assessing the risks to the rights and freedoms of citizens is critical to ensuring AI systems are used to benefit humanity.

If CoE's future legal framework encourages soft-law instruments such as codes of conduct, guidelines or certification mechanisms the ICO will welcome the opportunity to share its insights. We are in the process of collating views from industry about the operationalisation of our ExplAIn framework that could be informative for CoE.

The ICO is currently scoping work on the principle of fairness in the context of AI systems. It is important to note that DP law relates not just to DP but is also engaged in the protection of other fundamental rights such as the right to non-discrimination.

Bias and discrimination are increasingly important issues in the context of AI. As the Feasibility Study suggested, even when the statistical error rate of a system is close to zero, because of the scale of AI systems thousands of people may still be adversely impacted. It is therefore imperative to ensure any risks are minimised. We believe documentation requirements throughout the AI lifecycle will be crucial in that process, in the interests of both transparency and accountability.

In addition, we would like to make some comments about the main questionnaire. Firstly, we aimed to only respond to questions within the limits of our regulatory remit where we have specific policy positions.

We believe question 19 could profit from more clarity in terms of what is included in a "system". We would support a ban where there is a proven violation but we believe a risk assessed approach is needed that accounts for the context of use and where there is a risk to the rights and freedoms of citizens a precautionary approach can be adopted.

[9] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

For question 23 and as mentioned previously, we would like to note that the principles of transparency, explainability and non-discrimination are encompassed in DP. These principles and rights could be enhanced by strengthening or extending the current DP regime.

In regards to question 28, The ICO has found that data protection regulations have been flexible and capable of supporting the regulation AI systems in the context of personal data use. We recognise however, that the development and use of AI is evolving rapidly and may pose new risks that need to be addressed.

The scope of the sub-questions of point 32 was at times too broad for the ICO to provide an opinion. For instance, it may be impractical for individuals to always be informed when they interact with an AI system, in "any circumstances". A decision or a decision-making process may affect them "personally" but may, depending on the context, be trivial.

We believe putting the burden on individuals to be informed about every single algorithm-based decision would add to the administrative burden of companies and exhaust the scarce attention and time data subjects possess. On the other hand, individuals should have the means to "be informed" if they so wish, as GDPR's transparency principle dictates.

The ICO supports responsible innovation and wants to continue to ensure any enhanced or new regulatory regime is not an end in itself, and instead enables innovative use of data in technologies like AI by fostering the trust necessary for their use.

We also welcome the approach taken by the AI Guidelines of the Committee of Convention C108 and call for the principles contained in these Guidelines to be reflected in a future instrument. We finally refer the CAHAI to the 2021 Profiling Recommendation of the Committee of Convention C108.