8 October 2024

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Brussels Privacy Symposium 2024

Speech by;

Wojciech Wiewiórowski
European Data Protection Supervisor

Brussels Privacy Symposium

I. Introduction

Thank you to the Future of privacy Forum for inviting me to this conversation with Professor Gloria Gonzàlez Fuster.

Unfortunately, I was not able to take part in today's discussions due to other commitments, but I understand that the discussions were fruitful and interesting.

I can assure that the questions raised during the event were not only exciting but also very relevant to the current debates about the future of data protection law.

The debate around Artificial Intelligence is not only fascinating, but sometimes also not always easy to grasp.

The AI act of course, but also the GDPR but also the DMA and the DSA, are trying to regulate the same phenomenon but from a different angles.

The multiplication of the regulations to which AI systems are subject can make it difficult to understand under which conditions Ai systems can be legally used, that is to say that legal certainty has to be provided around the use and development of AI tools.

The complexity of the regulation can also make us forget what is at stake here: what is the AI Act really regulating? What are the core issues to be addressed?

Of course, risk, sensitive data, but also enforcement, covered by the three panels today, are of the essence to understand the digital landscape that we have to navigate.

However, we should not forget the main objective of digital regulations such as the AI Act: it is not only boosting innovation and ensuring the free movement of AI-based good and services, but also promote a human centric and trustworthy AI protecting the fundamental rights enshrined in the Charter of Fundamental Rights.

Let me use other words that are not usually used in this debate: it seems sometimes that we are asked to choose between artificial intelligence and human stupidity.

The debate is not as simple: AIs may be intelligent (not in a human way, of course) but is not human. Human can be stupid (but usually not) but they still are human.

I believe that this human dimension must be at the heart of our thinking about AI. Part of it is what we call "human in the loop". Because human dignity and rights will never be better defended than by humans, and because AI also will remain ignorant about fundamental rights if we don't feed the AI with our values.

Let me cite this example of the excellent British comedy show “Little Britain”, which you probably know. One recurrent scene is the one where a desk clerk use their computer in many situations, such as travel agencies, hospitals, and answer to the requests of the patients and customers with the famous answer “computer says no”.

This sketch even describes a famous catch phrase in the British culture used to criticise public-facing organisations and customer service staff who rely on answers generated by a computer to make decisions and used them to respond to customers' requests, often in a manner which goes against common sense, without possibility for the costumers to challenge or even understand the logic, should there be any logic involved.

That’s is in my opinion, exactly what we should aim at: try to address “computer says no” situations, where not only we as individuals impacted by the decisions of algorithms cannot challenge them, but where the human on the other side, using the AI, is not even in a position to change the outcome given by the machine.

When regulating AI, we should always keep in mind that “to err is human”, but also that computers can also fail.

That being said, let me go through the three main discussions that took place today to identify where I think that we should ensure that digital regulations correctly address AI and how we can build a bridge between the different regulatory regimes to make it workable for innovation, human rights, but also for regulators themselves.

II. On the risk in AI and Data protection

As already said, fundamental rights risks assessment is not new to data protection: the Data Protection Assessment in the GDPR can be used as a basis for building a Fundamental Rights Impact Assessment under the AI Act for High-Risk AI. Data Protection Authorities already provided guidance on how to conduct such an assessment, which both an internal compliance tool for organisations but also a useful document for regulators and potential enforcement.

Under the EU AI Act, the conformity assessment is designed to ensure accountability by the provider with each of the EU AI Act’s requirements for the safe development of a high-risk AI system.

The DPIA, on the other hand, is a mandatory step required from the controllers under Article 35 GDPR when the processing is likely to result in a high risk to the rights and freedoms of natural persons.

The AI Act explicitly refers to this obligation, by mentioning in Article 29(6) of the AI Act that users of high-risk AI systems should use the information as received from the provider, to carry out DPIAs, since a high-risk system often processes personal data. In such case, the technical documentation that are drafted for conformity assessments may help establishing the

factual context of a DPIA. Similarly, the technical information may be helpful to a deployer of the AI system that is required to conduct a DPIA in relation to its use of the system.

Furthermore, according to Article 27 of the AI Act a fundamental rights impact assessment "FRIA" shall be conducted before a high-risk AI system is deployed. Article 27(4) AI Act states that if any of the obligations laid down in this article are already met through the DPIA, the FRIA shall complement that DPIA. Therefore, the FRIA's content is broader than the DPIA. The FRIA should also take into account the specification of fundamental rights via the applicable sectoral laws (e.g. labour law).

Another example is Article 34(1)b of the DSA addresses the "actual or foreseeable negative effects for the exercise of fundamental rights. The DSA therefore also creates the need for a Fundamental Right Impact assessment (FRIA) for VLOP and obliges them to mitigate the risks identified. However, no guidance is provided to VLOP in this respect, although some documents such as the one suggested by civil society organisations.

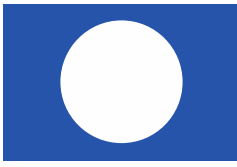
However, all these assessments must not become a pure box-ticking exercises, and it is of utmost importance to assess and review the assessments made by the organisations involved in AI, subject to the GDPR, or the VLOPs, knowing that some of them will be subject to each of these regulations.

Regarding the interplay between the AI Act and the GDPR: let me be clear: as I already said at other occasions, the mere qualification of an AI system as "high-risk" does not mean that its deployment is lawful, even if the specific safeguards imposed by the AI Act are implemented.

Instead, such qualification indicates a need for greater scrutiny, including from the perspective of EU data protection law where personal data are being processed. Annex III to the AI Act explicitly refers to AI systems "insofar as their use is permitted" (by Union or national law). The EDPS has significant doubts that certain uses of AI - which are merely classified as 'high-risk' - could meet in practice meet the requirements of necessity and proportionality in data protection law (even if the legislator failed to provide for explicit prohibitions).

On the other hand, minimal risk is unregulated by the AI, such as recommender systems. But this does not mean that they are not regulated by other laws, such as the DSA or even the GDPR since recommender systems

- use personal data and profiling, making GDPR applicable
- profiling is also regulated by the DSA which prohibits providers of online platforms from targeting ads on the basis of the special categories of data specified in Article 9(1) of the GDPR, such as sexual orientation, ethnicity or religious beliefs.



As a data protection authority, we have recommended, both as EDPS and as member of the EDPB, the prohibition of a number of AI uses. Some of them, for instance social scoring by both public and private authorities, have been banned under the AI Act (having regard to deployment, but not to development).

However, some other uses of AI, notably remote biometric recognition in public spaces, emotion 'recognition' (including for law enforcement, to 'predict' and so prevent future criminal offences), predictive police based on profiling, are considered as 'high-risk' in many cases, without being subject to a blanket prohibition. My recommendation in this regard is to carefully consider the interference on the fundamental rights and freedoms of such measures, on the one side, and the effectiveness, on the other hand. But first, whether the very essence of fundamental rights (not only to personal data but also to dignity) are not compromised.

It is crucial to recognize that the use of AI systems, entailing - in most cases if not always - the processing of personal data, will have to comply with the provisions of the AI Act. However, it's equally important to acknowledge that existing data protection legal framework - the GDPR and LED, ePrivacy, and the EUDPR - will continue to apply. Therefore, it is imperative for AI systems to adhere to data protection rules and principles (notably the requirements of necessity and proportionality).

In this respect, the EDPS has already issued guidelines on the use of Generative AI in June 2024, and actively contributes to the work of the EDPB regarding the interplay between the AI Act and the GDPR, but also on the recent opinion requested by the Irish Supervisory authority regarding compliance with the GDPR of the training of AI systems with personal data.

Regarding the place of the human in the AI systems: Article 14 EU AI Act requires high-risk AI system to be designed and developed in such a way (including with appropriate human-machine interface tools) that they can be effectively overseen by natural persons during the period in which the AI system is in use. In other words, providers must take a "human-oversight-by-design" approach to developing AI systems.

This requirement can contribute to ensure that the decision-making is not solely based on automated means or to ensure that the right of the data subject to obtain human intervention from the controller is provided, as required by the GDPR. At the same time, human intervention is not a 'silver bullet': it is a necessary requirement but by itself not sufficient to address all the risks of AI systems. However:

- First, the AI system should (regardless of human review) be compliant with fundamental rights;
- Second, in case a vast number of decisions is automated, human review might have only a limited role to play;
- Third, the human reviewer is still a person (the frontline staff) within the entity deploying the AI and therefore may have limited 'voice' to contest the

overall functioning of the AI. More to the point, human review cannot really operate when the AI is opaque.

III. On the use of sensitive data

The EDPS has concerns regarding other AI systems based on the processing of biometric data (for instance, face or voice), and, in particular, inferring 'orientations' or 'state of mind' or possibly anti-social intentions, from such biometrics. These systems are referred to in the AI Act as emotion recognition and biometric categorization systems.

Such systems remind us of a pseudoscience unfortunately popular in a dark period of European history, and known as physiognomic or phrenology. I am concerned that acritical uptake of those systems might provoke an unfortunate revival of discredited 'theories' whose 'implementation' would be a serious threat to the harmonious life of our society and fundamental rights of individuals.

Against this background, as EDPS I recommended a cautionary approach on the deployment of certain AI systems as I continue to have serious concerns for instance as to the necessity and proportionality of the deployment of remote biometric identification systems (namely, facial recognition) in public spaces in Europe.

It should be reminded that the use of sensitive data is strictly regulated by the GDPR but also by the DSA

Having regard to the prohibitions, notably the one under Article 5(1)(e) AI Act, I would like to flag the recent decision by the Dutch DPA on Clearview AI on the unlawfulness, regardless of its use, of the biometric identification system Clearview AI. In this case, the very establishment of the biometric database is considered in breach of the GDPR.

IV. On the governance and enforcement

Regulators from different fields and perspectives will have to work together to effectively prevent harms generated or amplified by AI. **Synergies between consumer, privacy, competition, AI governance, sectoral laws and digital services regulations will need to be explored.**

In all those Opinions, but also in the EDPB's 2021 Statement on the Digital Services Package and Data Strategy[1], DPAs have emphasized the need for robust supervision and clear

[1] *https://www.edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf*

roles for oversight authorities under the different parts of the EU Digital Rulebook, as well as the establishment of institutionalized and structured cooperation among relevant competent authorities.

Despite recommendations from the EDPS and the EDPB to make DPAs the supervisory authorities under some of these Proposals (like the DGA, the Data Act and the AI Act), or to give them a prominent role in coordinating with other authorities, this has not fully been taken up by the EU co-legislators. There are exceptions, like the Data Act, that makes DPAs competent when processing of personal data is at stake. In some instances, EU Member States may also decide to allocate enforcement responsibilities to DPAs (e.g., under the DGA and the AI Act), but from what we have seen so far, this has seldom been done[2]. This is concerning, since processing of personal data is central to the activities of the entities covered by each piece of the EU Digital Rulebook.

Even before the GDPR and any of the "digital" acts of the previous EU legislative mandate were approved, the EDPS was already stressing the importance of cross-regulatory dialogue between data protection, consumer protection and competition authorities for coherent enforcement of EU law in the digital age. In 2016, it proposed the creation of the **Digital Clearinghouse** as a voluntary network of regulatory bodies to share information, voluntarily and within the bounds of their respective competences, about possible breaches of the laws applicable in the digital ecosystem and to align on the most effective ways of tackling them. The recent book commemorating the EDPS's 20th anniversary provides a nice summary of the establishment and the activities of the Digital Clearinghouse, which functioned between 2017 and 2021[3].

With the emergence of many new rules and regulators from the EU Digital Rulebook, ensuring regulatory consistency has become even more important. Initiatives like the creation of the DMA High Level Group, where various European regulatory networks and bodies gather to converge towards consistent transdisciplinary approaches, shows that the idea of the Digital Clearinghouse is, today, more pertinent than ever. Setups similar to the Digital Clearinghouse are now surfacing at national level within and beyond the EU, for example in the Netherlands, France, Germany, Ireland and the UK4.

To help promote effective and coherent enforcement in the digital world, the EDPS will publish, later this year, a position paper on the future of cross-regulatory cooperation entitled

---

[2] *See, for the DGA: https://ec.europa.eu/newsroom/dae/redirection/document/98966; for the DSA: https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs. DPAs have been pushing for becoming national competent authorities under the AI Act (see statements from the EDPB, CNIL and NL SA).*

[3] *Chapter (15) 'A clear imbalance between the data subject and the controller': data protection and competition law', by Christian D'Cunha and Anna Colaps, in the book 'Two decades of personal data protection. What's next?', EDPS 20th Anniversary.*

[4] *NL: https://www.acm.nl/en/about-acm/cooperation/national-cooperation/digital-regulation-cooperation-platform-sdt; FR: Article 51 of Loi n°2024-449 added Article 7-2 to Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ; DE: https://www.digitalclusterbonn.de/DCB/PM1.pdf?__blob=publicationFile&v=4; IE : https://www.ccpc.ie/business/wp-content/uploads/sites/3/2023/08/2023.06.29_CCPC_Annual-Report-2022.pdf; UK : https://www.drcf.org.uk/__data/assets/pdf_file/0030/258573/DRCF-Terms-of-Reference.pdf.*

"Towards a Digital Clearinghouse 2.0"[5]. On 24 October, the EDPS is hosting a stakeholder event to discuss the position paper and the way forward to ensure a coherent approach to regulatory cooperation in Europe's digital sphere.

We are still finalising the paper for publication, which will also feed on the inputs we will receive during the stakeholder event. But we already know that, at least, a DCH 2.0 should provide a forum for interested regulators to identify emerging areas of cross-regulatory concern, facilitate coordination and to exchange knowledge, experiences and resources. We also believe that, for the success of the Digital Clearinghouse 2.0, having a central body with enough resources providing a secretariat would be quite important, taking the example we see in the UK. It is also key that no single authority acts as the agenda-setter, and that all concerned regulators are effectively able to contribute on an equal footing to the conversation. In an ideal world, the central body coordinating the Digital Clearinghouse 2.0 would be established in law also setting out its objectives, role, and resources.

The **EDPS has been given the task to monitor EUIs' compliance with the AI Act**. In essence, the EDPS will act as notified body, notifying and market surveillance authority (MSA) to assess the conformity of high-risk AI systems that are developed or deployed by EUIs. The EDPS will also act as competent supervisory authority for the supervision of the provision or use of AI systems by EUIs. The EDPS has started the internal work to be ready to supervise AI systems.

The EDPS **welcomes the establishment within the Commission of the AI Office**, which has the mission to help Member States cooperate on enforcement, including on joint investigations, and acts as the Secretariat of the AI Board, the intergovernmental forum for coordination between national regulators. While the EDPS has only been given the status of "observer", he intends to contribute actively to the activities of the AI Board in order to promote the effective and consistent application of the AI Act.

The EDPS considers that national DPAs would be uniquely placed to enforce AI Act provisions, also beyond the supervision of the high-risk AI systems mentioned in Article 74(8) AI Act. Designating DPAs would allow leveraging synergies with enforcement of privacy and data protection principles and laws as expression of fundamental rights. In any event, it is important to recall that the oversight of GDPR and LED (and EUDPR, in case of EDPS) remains entrusted to data protection authorities, whose competence is not affected by the AI Act. The substantive provisions and principles of data protection are also not affected by the AI Act (as expressly mentioned by the AI Act.

Legal certainty on the interpretation of the AI Act is of paramount importance, also for the EDPS as enforcer. The EDPS hopes all regulatory actors involved will contribute to such legal certainty, for instance via guidelines that ensure compliance with the AI Act and effectively uphold protection of fundamental rights instead of decreasing the level of protection.

[5] https://20years.edps.europa.eu/en/initiatives/towards-digital-clearinghouse-20.

In this respect, the institutionalisation of sandboxes, where AI tools can be tested in "a safe environment" with the regulators, will be an interesting tool for AI deployers to be tested. Supervisory Authorities should however make sure to keep their independence.

Last but not least, let me also mention the **Collective Redress Directive**, adopted in 2020, which will create the path for class action styles cases filed by consumer organisations and civil society, and where not only the GDPR, but also all other laws of the EU digital rulebook, including the AI Act, can be invoked in court. These kind of actions will not only defragment any action brought into court since several EU digital legislations will be debated by one court (vs several regulators) but will also foster enforcement, since it will not only depend on the action by the regulators in charge of enforcing the legislation.