23 September 2024

International Organisations Workshop on Data Protection Washington DC (USA), World Bank premises

Keynote speech by;

Wojciech Wiewiórowski
European Data Protection Supervisor

EDPS

EUROPEAN
DATA
PROTECTION
SUPERVISOR

The EU's independent data protection authority

2004
2024
EDPS

International Organisations Workshop on Data Protection

I. Introduction

Thank the co-hosts from the World Bank

I am extremely happy to be here, in Washington DC, for the first edition of this event outside Europe, in the headquarters of the World Bank.

The EDPS turned 20 this year and the Workshop will turn 20 next year. This means that after just only one year of existence, the EDPS, at the time a small institution with a few employees - and as the DPA of a sui generis international organisation, the European Union -felt the need to engage with international organisations as one of its first cooperation actions.

I am actually extremely proud and supportive of this initiative. Do you know why? Because as data knows no borders, neither do rights. I am deeply convinced that international cooperation is necessary to ensure the protection of individuals, regardless of where their data are being processed. International organisations are key partners and stakeholders in this endeavour. Today, like my predecessor Peter Hustinx 20 years ago, I feel that we need this platform for international organisations. A platform where you, colleagues, can exchange knowledge, experience, and best practices and help our organisations advance in the field of privacy and data protection.

I have spent 10 years at the EDPS, and during this time, I have witnessed how this event - which started very small with a few people sitting around a table - keeps growing and attracting new colleagues and organisations. We are now gathering close to 150 participants per edition representing a wide range of international organisations.

This is a sign of the ever-stronger commitment of International Organisations to promote and ensure high data protection standards as a trust-enabler and as one element contributing to their credibility. And International Organisations like many organisations, including Data Protection Autorities, are stronger when they work together, when they exchange best practices - and when more members join the club.

You will have plenty of time during these two days to exchange and discuss - perhaps also sometimes to complain or criticise (don't be shy, sometimes we need that too)

But for now, allow me to share with you few thoughts on what I see as one of the most pressing challenges for our community. How can we ensure that the data protection principles are upheld along with the rise of Artificial Intelligence?

II. Data Protection and AI

Well, we would probably all agree that data protection and AI are heavily interlinked. And we will discuss later today how AI is impacting International Organisations. However, I would

like to kick off the discussion with a clear message: **Data protection and privacy will not merge, nor will they disperse into Artificial Intelligence.**

I am here today to defend data protection and privacy against the risk to dilute them into the AI hype. In fact, this could only mean dangerously weakening these fundamental rights. I said the same last month, when the AI Act entered into force and the EDPS officially became the AI supervisory authority for EU Institutions; The two must remain separate.

However, I am not naive, and you are not a naive community either. Of course, Artificial Intelligence is fuelled by data, much data that some operators refuse to recognise as 'personal' because (they claim) these data have been aggregated or anonymised. Artificial intelligence and data protection are different, and so are the legislative frameworks related to them. Let's take the example of the EU. The recently adopted AI Act is framed as an internal market legislation for commercialising AI systems. Therefore, it is something completely different from a tool like the GDPR, created to 'protect fundamental rights'. And, in this act, you will not find any answers on how to safeguard your privacy and data protection.

However, the EU AI Act also does not apply in a vacuum as it is part of a broader legal framework that contains provisions to protect individuals from the misuse of AI systems. Let me give you an example, the qualification of an AI system as "high-risk" in the AI Act does not mean that its deployment is lawful, even if the specific safeguards imposed by the AI Act are implemented. Instead, this qualification indicates a need for greater scrutiny, including from the perspective of EU data protection law, where personal data are being processed.

For now, in the EU, data protection has not turned into "everything AI". **Compliance with data protection and privacy rules is the essential prerequisite to put people at the centre, and ahead of technology.** That is why, **we must work together to defend the identity of data protection to protect humanity.** But how do we do that?

III. Towards a Digital Humanism

In my opinion, we need to bring **human dignity** to the centre of the discussion on AI. For as much as the law can provide for permitted vs. banned uses of a certain technology, the law will not always draw a specific line of '**what is right**' from '**what is wrong**'.

The world of Artificial Intelligence is controlled, as many others in the digital realms, by a very limited number of large companies. They are the ones having the ability to develop and deploy AI at scale, and they make decisions with a crucial societal impact on humanity. However, we, as the rest of humankind, are not part of any relevant decision-making.

Colleagues, in order to solve this duality, we must embark on a **profound rethinking** of market structure of technology and the accumulation of power that comes from it, as these have a direct impact on people's fundamental rights, including the right to privacy and data protection. EU legislation, such as the Digital Markets Act, the Digital Services Act and the likes, will certainly help. They are already advancing the cause of protecting rights of people. But these

acts cannot achieve any fundamental rethinking of our Digital World. **We must devise the trajectory for a future, which can be just and fair to everyone.**

Digital Humanism cannot be built on **digital artefacts** such as AI systems, possibly deployed on large scale, that run counter to **the values of liberal democracies.**

These values, at the end of day, find their root in the overarching principle of **human dignity**, as enshrined in Article 1 of the Universal Declaration of Human Rights. This principle (dignity) is also at the root of the **fundamental rights to privacy and to the protection of personal data.**

Now, how can we translate this in practice? As EDPS, I recommended a cautionary approach to the deployment of certain AI systems. I have serious concerns, for instance, about the **necessity and proportionality** of the deployment of **remote biometric identification systems (namely, facial recognition)** in public spaces in Europe.

I also have concerns regarding other **AI systems based on the processing of biometric data** (like face or voice), in particular, when AI automatically infers '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 systems and biometric categorisation AI systems.**

Another important threat, that I am sure you are fully mindful about, is **the threat to democracy** represented by **fake news, images and video. The creation and circulation of this content is facilitated by artificial intelligence systems known as generative AI systems.** The fact of not being able to tell what is true from what is false is already a matter of concern. But the use of such content for political advertising and propaganda is even more concerning, as it undermines the very pillars of democracy. Imagine what damages a large deployment of AI generated fake news could bring. It could tear apart trust in society. That is why discussions on how deepfakes and disinformation will play out in elections and the democratic process are increasing in intensity.

Finally, I would like to talk about the future, our real future, our **children**.

Artificial intelligence systems should represent an opportunity, not a threat for the new generations.

I am a father, so I feel the moral obligation - as I believe do everybody in this room and online - to respect the mental integrity of our children and support their autonomy. That is why we must do better! We need to make sure that we provide them with healthy online tools. Tools that are enriching their lives, allowing them to develop into free-thinking adults and helping them integrate in our society. Whether and how our sons and daughters are subject to AI systems should be guided by the fundamental principle of their best interest.

Colleagues, friends, as you can tell, the stakes are high. Thus, it is important that we all work together to help our children to develop a **healthy relationship with technology**. And this also means setting **healthy boundaries around its use.**
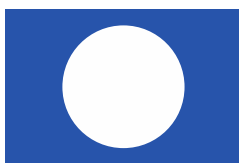
IV. Conclusion

I just shared few thoughts even though I could go on for hours; I see that I am now running out of time. So allow me to do a quick wrap-up:

Colleagues, the challenges we are facing are huge and will probably be even greater tomorrow. I am convinced that ensuring a safe digital environment will very much depend on how we rein in on the development and deployment of AI systems.

I have no doubts that International Organisations are and will be not only heavily impacted by these technological changes, but will also play an important role in governing these changes.

This is why - once again - I am convinced that we need this platform to share our common challenges, and ultimately to discuss and explore common solutions.

Thank you for your attention and let me wish you a productive and successful workshop.