Towards a New Digital Ethics: Data, Dignity and Technology

Speech before Institute of International and European Affairs

Dublin , 8 October 2015

Giovanni Buttarelli

A very warm thank you to the Director of Research, Jill Donoghue and the IIEA for their invitation to speak to you today.

The work of the Institute as a thought leader in politics and international relations is impressive, and it is a great honour to be here.

I have been in the business of regulating personal data processing for over 20 years.

Moreover, for most of that time data protection has been treated as a technical abstraction on the margins of political discourse.

Yesterday a ruling by the EU Court of Justice, on a case concerning a not so well known Commission decision about data sharing, on a referral from the High Court here in Ireland, made headlines in every major news outlet around the world.

I do not recall EU data protection ever commanding such a level of global attention.

So the timing - and location - of this discussion is impeccable.

I am convinced that we are now at a crossroads: a point in time where law, technology and public opinion seem to converge around a set of core principles and values.

I do not intend to speak at length about the demise of Safe Harbor. For me, and I suspect for many of the experts closely associated with the case in this room, the judgment was not a big surprise.

The Schrems case needs to be situated in distinct cycle of jurisprudence that has put living flesh on the sturdy skeleton of the Charter of Fundamental Rights. Legislators, governments, businesses and citizens can be in no doubt about that the rights to privacy and to data protection are important and cannot be ignored.

I'd like to touch on three aspects of the digital ethics which we want to promote, which draws on our opinion published last month, and on several observations from my recent trip to Silicon Valley.

First, what is the ethical dimension to data processing and why is it important?

Second, what might a digital ethics look like?

Third, how do we build a consensus to get there?

Let me begin with a brief overview of the institution I represent.

The EDPS is an independent institution of the EU, and, like the organization which Helen Dixon here in the audience leads, an independent data protection authority.

We are responsible under European Union Regulation 45/2001 for monitoring and enforcing compliance with data protection standards in all EU institutions and bodies, agencies and offices, large and small. And we are responsible for advising EU institutions, like the Commission and Parliament, on all matters concerning the processing of personal data'.

The Assistant Supervisor and I were appointed in December 2014 with the specific remit of being constructive and proactive.

That is why we published in March 2015 a five-year strategy. It was our vision for the EU to be a beacon of best practice and forward thinking on treating people and information about them with respect, and being accountable.

As with the 18th and 19th century industrial revolution and the genesis of the human rights movement, there is a similar imperative now to safeguard dignity in the digital revolution.

Ethics is an established factor in medicine, and it is driving notions of corporate social responsibility and environmental responsibility towards future generations.

Scientists and entrepreneurs are realizing that the explosion of personal information and power of computers, AI and virtual reality, raise profound questions.

Questions about what it will mean to be human in the future, who should be responsible and liable for decisions that affect people in their daily lives when we are all using similar platforms and devices.

Even the Pope himself has written about the 'mental pollution' of the 'mere accumulation of data' divorced from genuine human exchange and self-reflection.

In practical terms, we see it now in cloud services – where there is a general reluctance for anyone to take responsibility for what happens to the data – nobody wants to hold the encryption keys.

Many data controllers claim they simply do not know where the data is.

Surveillance is the business model of the internet – most people have not subscribed to this.

The EU in its Digital Single Market strategy seems to be tempted to import the West Coast approach where there is no principle of data minimization or of purpose limitation, where any obstacles to data flows are considered bad for innovation

Meanwhile there is a security ratchet, where it is now assumed that law enforcement and the security services must, to keep pace with terrorists and cybercriminals, simply store indefinitely and indiscriminately all data available.

We saw this with data retention. We see it now with PNR.

Security - which used to be a concept closely connected to privacy (sine cura), is now deliberately left vague and undefined, so that it can be used to justify more and more intrusions into the private lives or more and more people.

An ethical approach looks at the longer-term implications for society and the individual of these trends, and seeks to identify new norms to prevent unintended consequences.

Our 2015 ethics opinion outlined what we called a big data protection ecosystem, an interdependency consisting of regulation, businesses and organisations processing information, engineers and designers, and individuals themselves.

It was a recognition that good laws are necessary but insufficient.

Controllers need to be aware of and accountable for the impact of their business decisions on individuals. The Google Spain judgment, for example, rebutted the defendants claim to be merely indexing impartially the information placed online by content providers.

In fact, Google were not providing a public or charitable service. They were making business decisions, using algorithms driven by their legitimate business interests.

And these legitimate interests cannot take precedence over the fundamental rights of the individual concerned by the data.

Technology is not value neutral. It is the result of human ingenuity and reflective of the value system of those men and women.

It is only now that people are beginning to realise the prescience of Lawrence Lessig's declaration, around 15 years ago, that 'Code is Law'.

In order words, the rules and standards that are devised to govern cyberspace, like the anonymity or traceability of individuals, are at least as powerful as the formal legal framework applied by the courts.

The problem is that the internet that has emerged was devised by brilliant scientists and technicians. But these brilliant people did not necessarily understand or reflect on fundamental values like human dignity, privacy and freedom of expression.

We are starting to change that, by bringing together legal experts and engineers. This will be crucial to the long-term sustainability and competitiveness of the digital single market in the EU.

Finally, we need empowered individuals who are not just treated as passive data subjects vulnerable to exploitation and requiring protection.

People are prosumers of content online, and structures must be put in place to address power and information imbalances.

We aim to give a kick-start by pulling together a data protection ethics advisory board. It will operate transparently, be a resource for the EU generally, and include visionaries from outside the data protection community.

Data protection authorities will play a crucial role, because they alone have the resources and expertise to grapple with a very technical area of law.

For this, their independence must be protected and their capacity for forward thinking enhanced.

They must be trusted to cooperate in the EU, which means they must be free from unnecessary prescriptive procedures in the GDPR.

Perhaps most importantly, we need to build bridges with other regions and countries where values are shared.

The focus this week is on the EU and the US – 'The Atlantic just got wider' – wrote one commentator (Guardian) on Wednesday

But in fact we have a great deal in common.

And if we can reach a common understanding it can be a platform for the rest of the world, where there are now over 110 countries with data protection laws, outnumbering Europe for the first time.

So this is the challenge. I look forward to our discussion.