CommDH/Speech(2019)14

"Governing the digital world to protect democracy and security"

Speech by Dunja Mijatović
Council of Europe Commissioner for Human Rights

OSCE Security Days
A Human Rights-centred approach to Security and Technology

Vienna, 8 November 2019

Thirty years ago, tomorrow, crowds of East Germans crossed the border peacefully and climbed on the Berlin Wall together with West Germans. That symbolic moment, which catalysed months of civil unrest in Eastern Europe, told the world that a new era had just started.

Over the past thirty years, our European family has become bigger, freer, safer and more democratic. We have certainly gone far during this recent past. But not far enough. Aggressive nationalism, economic difficulties and terrorism are fomenting new tensions and polarisation. This is something that our continent has already experience. What is new is that technological development is being used as an accelerator of these phenomena and elevates their ability to undermine security and the democratic fabric of our society.

In an era when humans and machines are living in an ever-closer relationship, ensuring that technological development works for and not against human rights, democracy and the rule of law is one of the biggest tasks that States must face.

Indeed, technology is never neutral. It is very personal because it carries ethical, political and legal implications. Digital technologies can improve the quality of our lives, increase efficiency, strengthen accountability, create new opportunities in many key sectors of life like health care, education and employment. And it can of course strengthen human rights protection in a variety of ways. So far, digital development has mainly turned against users, perpetrated injustices and restricted people's rights.

A case in point is privacy. Large amounts of personal data is collected - with or without our knowledge - and are used to profile us. We provide data on our health, political ideas and family life without knowing who is going to use this data, how and why.

Another alarming phenomenon is the cozy relations between technology companies and state security agencies, which has grown stronger as part of states response to terrorist threats and attacks. States around the world have increased their surveillance arsenal, not always to the benefit of our safety though. On the contrary, in several occasions they used it to silence criticism, restrict free assembly, snoop into our private life, or control individuals or minorities.

Within the digital revolution, artificial intelligence is probably the sector that has expanded the most, without due regard to human rights. There is a great amount of evidence that women, older people, minority groups, people with disabilities, LGBTI and economically disadvantaged persons particularly suffer from discrimination at the hands of biased algorithms.

Sometimes AI causes harm because developers and users are too confident about the powers of machines. In other cases, however, there are more conscious decisions to use AI's potential to reinforce stereotypes and consolidate political, social and economic power in the hands of a few.

Digital technologies are in fact very often used to manipulate public opinion. There is no lack of evidence that disinformation, incitement to hatred and violence have been propagated by tricking the algorithms of some social media platforms, including by using bots and fake accounts. This has contributed to instilling fear in the population and pushing the frames of anti-democratic movements and extreme right-parties in particular in connection with election or referendum days.

We cannot allow this digital Far West to continue. Governments must retake control. The good news is that they do not need to reinvent the wheel. They already have the tools and the knowledge to ensure that technology benefits and enhance human rights protection.

The Recommendation on Artificial Intelligence that I published in May can be used to that purpose. It is based on existing standards and on work done in this area by the Council of Europe and other international organisations. It aims to guide member states to maximise the potential of artificial intelligence systems and prevent or mitigate the negative impact they may have on people's lives and rights, focusing on 10 areas of action.

One such area relates to the obligation of governments to ensure that business enterprises abide by human rights standards. Self-imposed standards can be useful, and several businesses are already implementing them in good faith. But they are not enough. Standards vary across the globe and voluntary commitments are unlikely to prevent the negative effects of bad business practice on human rights. Since States bear the responsibility to respect, protect and fulfill every person's human rights, it is their duty to ensure that private companies which design, develop or use AI systems do not violate human rights standards.

This can happen by engaging more resolutely with tech industries to make them aware of the necessity to incorporate human rights in the design of AI systems and push them to assess the human rights impact of these systems. A more inclusive cooperation among state actors, the private sector, academia, NGOs, the media and citizens' groups would greatly help in this sense.

States should also reinforce their monitoring of human rights compliance by AI systems and act anytime there is an infringement of these rights. They should strengthen independent oversight and empower national human rights structures to engage in this field too. It is crucial to keep human control and human liability in relation to AI.

Finally, States should promote digital literacy among the population, and in particular in schools, in order to help people understand how the digital world works and recognise when it harms. For this to happen, States should invest more in public awareness, trainings and education initiatives to develop the competencies of citizens and address the knowledge gap. It may be a costly investment but with a huge democratic return.

At stake is the society we want to live in and pass it on to the next generations. Digital technologies can strengthen our freedoms or oppress them. They can bolster participation or become a threat to democracy. They can empower people or push them at the margin of society.

It is up to us to steer them, not the other way round.