Technology Decalogue (not only) for Coronavirus Times

or

Modern technologies go hand in hand with human rights even in emergency situations

The document has been prepared by the *Working Group for Human Rights and Modern Technologies of the Government Council for Human Rights* which joins experts from the state, academic, non-profit and private sectors in the field of human rights and modern technologies. These experts warn about the cases of potential and actual violation of human rights related to the use of modern technologies at the time of the coronavirus epidemic. Their discussions resulted in ten measures intended for persons involved in the public and private spheres, which, in the opinion of the Working Group, would help the current situation or can be useful in the future.

1. Technology and digitization have proven to be crucial in the age of coronavirus. It is therefore appropriate to continue their implementation across sectors (e.g. in the areas of telecommunications infrastructure, e-government or distance learning). The use of technology must be accompanied by appropriate financial support and training for those who are to work with it (both public authorities and users). Contributing to the development of digitization is primarily the task of public administration. Technological measures that have been put in place during a crisis situation and that have proved their worth without adversely affecting or contributing to observance of human rights should be maintained.

2. During emergency situations, the functioning of judicial and administrative authorities must be ensured, in particular with the aim not to prolong the length of proceedings beyond the tolerable limit. It is necessary to look for the possibility of using modern technologies that would enable these bodies to function properly and continuously. Above all, these solutions must fulfil the right to a fair trial.

3. Even in emergency situations, existing tools and processes may not be used for a fundamentally different purpose than for which they were originally created, such as monitoring or profiling the population. It is not possible to collect excessive amounts of data and to interconnect data in registers in a way that would significantly alter their previously determined purpose. Similarly, excessive surveillance of individuals, invading privacy and dignity, is unacceptable.

4. Emergencies are not an excuse for non-compliance with data protection rules. On the contrary, in connection with greater use of technological tools the importance of this protection is growing. Emphasis must be placed on the transparency of data processing and its compliance with privacy and personal data protection rules, as well as non-discrimination. It is necessary to analyse the current handling of personal data at the time of emergency situations in order to learn from mistakes and shortcomings.

5. Simultaneously with the introduction of modern technologies and procedures, it is necessary to ensure that their addressees can use them. An unsecured connection, equipment or lack of digital skills can lead to the exclusion of certain groups from participating in social life (seniors, people with special needs, pupils educated from home, single parents, etc.). Also entrepreneurs may face similar problems for the same reasons.

6. Information transmitted via technologies must respect all addressees and adapt its form accordingly (e.g. conversion to sign language or adaptation for the visually impaired and the blind). And there should be a non-digital way of communication for those who cannot or do not want to use modern technology.

7. Access to information is crucial, especially in crisis situations. The media should adhere to the professional and ethical standards of responsible journalism and publish only verified information. Stigmatization of victims of crisis situations or unjustified association of certain social groups with the ongoing crisis should also be avoided. The government should function openly, provide relevant information to the media in a comprehensible and accessible form, and not conceal key facts, but also not spread panic. The government must not resort to censorship.

8. The use of modern technologies in solving crisis situations must always be accompanied by a clear, convincing and uniform explanation of their meaning and objectives. Above all, the addressees must understand and have confidence in the measures on the basis of facts, transparent communication and expertise. The accompanying phenomenon of today's society is an increase of disinformation, conspiracy theories and attempt to relativize facts, which threatens solution of the crisis situations. The government and the media should therefore jointly aim to raise awareness in the society and provide guidance on the use of modern technologies to successfully manage crisis situations.

9. Employees of public and private sector should be trained in cybersecurity and the rules of safe work from home/online. The training should be beneficial for the employee concerned and respond to current threats in the area concerned. It is advisable to test the acquisition of necessary knowledge in order to identify possible training deficiencies. Private companies and public institutions should monitor and increase the security of their networks, suppliers of equipment, services and software accordingly.

10. Employers should, as far as possible, make greater use of flexible forms of work for their employees, in a mutually beneficial form, in order to achieve a better work-life balance and greater work involvement of the persons who take care of children or dependents. At the same time, flexible forms of work must not lead to violations of the Labour Code, especially in the schedule and observance of working hours. Employers and employees should also be trained in the use of flexible forms of work, including balancing online and offline life.