The COVID-19 pandemic (better known as the coronavirus) poses unprecedented threats and challenges to individuals and countries around the world. The need to stop its spread and heal those affected by it is a goal shared by people around the world.

The efforts of the World Health Organization, international organizations, governments, health institutions and their staff and businesses to prevent the spread of the virus on a large scale to save people and protect society are limitless and should be strongly supported.

In the context of democracy, states must face the threats posed by the COVID-19 pandemic for the rule of law and human rights, including the right to privacy and data protection.

In an effort to combat further new infections, governments have had to resort to emergency measures, including declaring a state of emergency in many cases. Although the alarming public health situation of these countries justified the introduction of special regimes, it should be emphasized that during these limited periods, the exercise of human rights, as set out in several international and national instruments (such as the International Covenant on Civil and Political Rights and the European Convention on Civil Rights). human rights) is applicable and cannot be suspended, but only derogated from or restricted by law, to the extent strictly required by the needs of the individual situation, respecting the essence of fundamental rights and freedoms.

General principles and rules of data protection

When it comes to the right to data protection, it should be noted that Convention 108, as well as the modernized "Convention 108+", set high standards for personal data protection that are compatible and compatible with other fundamental rights and relevant public interests.

It is important to recall that data protection can in no way be an obstacle to saving lives and that the applicable principles always allow for a balance of interests.

In accordance with Convention 108+, even in particularly difficult situations, it is crucial to respect the principles of data protection.

In this regard, it is crucial:

- ensure that respondents are acquainted with the processing of their data;

- process personal data only, if necessary, and in proportion to the explicit, specific and legitimate aim pursued;

- performs an impact assessment before processing;

- ensure technical and integrated data protection and adopt appropriate security measures for data protection, in particular for specific categories of data, such as health-related data;

- respondents have the right to exercise their rights.

One of the main principles of data protection provided for in Convention 108+ is the principle of legality, according to which data processing may be carried out either with the consent of the respondents or on some other legal basis. It should be noted that, as explicitly presented in the Explanatory Memorandum to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, such a legal basis includes in particular the processing of data necessary for the vital interests of individuals. which is the case with monitoring a life-threatening epidemic.

For example, the right to data protection does not prevent public health services from exchanging lists of health professionals (names and contact details) with entities entrusted with the distribution of FFP2 masks. Nor can it be argued that the right to data protection is incompatible with epidemiological surveillance, pointing out that anonymous data is not covered by data protection requirements. Therefore, the use of aggregate location information to signal gatherings that violate closure conditions or to mark the movement of persons traveling through large-scale pandemic-affected areas (in terms of the number of COVID-19 positives) would not be prevented by data protection requirements.

Furthermore, the "Convention 108+" confirms the need for permissible exceptions and limitations in the context of urgent objectives of public interest and the vital interests of individuals. However, the limitations of its principles and rights must meet very clear requirements, even during a state of emergency, in order to ensure lasting respect for the rule of law and fundamental rights.

According to Convention 108+ (Article 11), exceptions are "provided by law, respect the essence of fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society".

Where restrictions apply, those measures must be taken only temporarily and only for a period explicitly limited to the state of emergency. It is also crucial to establish special safeguards and the belief that personal data is fully protected after a state of emergency is lifted. This should include specific specific measures and procedures related to the return to the normal data processing regime, with particular attention to databases containing health data or other special categories of data and / or those created for the purpose of monitoring and profiling individuals processed. during a state of emergency.

Data protection authorities are invited to carefully assess the measures taken by public authorities in relation to these conditions.

Health data processing

Provided that the priority is a human being and that professional standards of guiding value are accepted in the field of health care, the processing of health-related data guarantees respect for the rights and fundamental freedoms of every individual, especially the right to privacy and personal data protection. In this regard, Recommendation CM / Rec (2019) 2 on health-related data provides specific guidance. Its provisions on the exchange of data, between health professionals and between health and other sectors, should guide the practice of individual professionals. A special chapter of the Recommendation is dedicated to scientific research, which is currently one of the key areas of international cooperation in the fight against COVID-19.

Informing the public about health and government bodies should continue to be a priority so that they can protect, inform and advise the general public. However, the publication of sensitive data (such as health-related data) of certain persons should be avoided during such reporting and it is recommended that such data be processed only if additional technical and organizational measures are taken to complement those applicable to non-sensitive data.

Large-scale data processing

As vast data and databases are generated, taking advantage of data processing techniques and technologies such as ‘Big data’ and artificial intelligence, this data should be processed in environments that respect human dignity and data protection. In the context of ‘Big Data’ and artificial intelligence, Convention Committee 108 has developed appropriate guidelines that can be useful tools for developers and governments in designing these treatments in a way that protects against abuse or unintended negative consequences, including discrimination against individuals or groups of individuals.

Transparency and “explainability” of analytical or artificial intelligence-based solutions, a precautionary approach and risk management strategy (including the risk of re-identification in the case of anonymous data), a focus on data quality and minimizing the role of human oversight are some of the key points to consider. consideration in the development of innovative solutions to combat COVID-19.

Data processing carried out by employers

At the same time protecting the public and their employees, employers face difficulties in maintaining their business or

activities, and especially when employees work remotely, through networks. However, this practice should not lead to employee surveillance, including video means; unobtrusive measures should be taken into account in the organization and working conditions.

Under the circumstances, employers may need to process personal or sensitive data that they do not normally process (such as health data); it should therefore be recalled that the principles of necessity, proportionality and accountability should be respected. They should also be guided by principles designed to minimize all risks that such processing may pose to employees' rights and fundamental freedoms, in particular their rights to privacy, as elaborated in Recommendation CM / Rec (2015) 5 on the processing of personal data in the employment context. In particular, employers should not process personal data other than what is necessary to identify potentially exposed employees.

If they are required by law to disclose certain information to public authorities for public health reasons, they are urged to do so in strict compliance with the basic legal basis, taking the necessary measures to return to "normal" processing (including permanent deletion) after the state of emergency is no longer applicable.

Mobile, computer data

Telecommunications companies, Internet platforms and Internet service providers are also actively involved in the fight against the spread of COVID-19, and they are increasingly obliged to share subscriber data, personal data collected and other types of information with public authorities. significantly contributed to epidemiological surveillance, including the analysis of spatial data to determine the location of potentially infected persons. Similarly, private and public bodies can develop IT solutions to control the epidemic.

Large-scale processing of personal data can only take place if, based on scientific evidence, the potential public health benefits of such digital epidemic surveillance (eg contact tracking), including their accuracy, outweigh the benefits of other less intrusive alternatives.

The development of these supervisory solutions should be based on a preliminary assessment of the likely impact of the intended data processing on the rights and fundamental freedoms of respondents, and data processing should be designed to prevent or reduce the risk of interference with fundamental rights and freedoms.

Given the principles of precaution and proportionality, it is recommended that prior testing be performed in different “boxes”, as is the case with the different possible drugs tested in clinical trials.

Although real-time information on the spread of the virus may be important for its isolation, it should be emphasized that the least intrusive solutions should always be preferred.

Data processing in educational systems

Schools and universities are making every effort to increase skills and resources for distance learning, and professors and teachers themselves face the challenge of isolation. When considering technical solutions aimed at ensuring the continuity of educational work, preference should be given to configurations oriented to data protection, for example in relation to default settings, so that the use of applications and software does not infringe on the rights of respondents. than is necessary to achieve the legitimate purpose of ensuring educational continuity.

Also, it is of primary importance to choose the appropriate legal basis (including parental or legal representation, if necessary) and to allow parents maximum transparency regarding the processing of their children's data.

Additional guidance on the processing of personal data, in the context of education, is currently being prepared by the Convention Committee 108 and will serve practitioners and decision makers.

**

As people face difficult and threatening times, as the situation develops rapidly and governments take measures to protect the population, they must do so without endangering society in the long run.

Only through unity and solidarity, with full respect for the rule of law, human rights and democracy, will we overcome this situation without prejudice.

Original text available at:

https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter