ديوان الموظفين العام
General Personnel Council

CDL-UD(2021)014

Or. Engl.

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW (VENICE COMMISSION)

in cooperation with

THE GENERAL PERSONNEL COUNCIL OF PALESTINE*

Regional seminar for high level civil servants

13th UniDem Med

"PUBLIC ADMINISTRATION FACING THE COVID-19 PANDEMIC: MODERNISATION AND DIGITAL INNOVATIONS”

Videoconference, Palestine*

5-6 October 2021

THE COVID-19 PANDEMIC AS AN ACCELERATOR OF DIGITAL INNOVATIONS AND DIGITAL TRANSFORMATION OF PUBLIC SERVICES: TOWARDS A MORE DEMOCRATIC, OPEN AND INCLUSIVE PUBLIC ADMINISTRATION

by

Mr Alessandro MANTELERO

(Associate Professor of Private Law, Department of Management and Production Engineering, Polytechnic of Turin, Italy)

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

The Unidem Med project is implemented in the framework of the European Union/Council of Europe joint programme
“Regional Support to Reinforce Human Rights, Rule of Law and Democracy in the Southern Mediterranean”
(South Programme IV)

Venice Commission - Council of Europe Commission de Venise – Conseil de l’Europe
F-67075 Strasbourg Cedex Tel. +33 (0) 3 88 41 38 23 Fax +33 (0) 3 88 41 37 38
E-mail: venice@coe.int Web site: www.venice.coe.int

*This document has been produced as part of a programme co-funded by the European Union and the Council of Europe.
The views expressed herein can in no way be taken to reflect the official opinion of either party.*

[*] This designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of Council of Europe and European Union member States on this issue.

The role of Convention 108+ in a human rights-oriented digital and innovative public administration

Alessandro Mantelero[*]

1. The scenario

The increasing use of data and data-intensive systems over the last decades, as well as the advent of the new wave of AI, have provided a large number of opportunities and benefits for citizens in terms of more efficient public administration, personalisation of public services, reduced costs, transparency and access to information.

However, digital technologies – like all technologies developed over the centuries by human beings – can also entail challenges and side effects in case of misuse, unintended consequences, etc. The recent case of the biometric database created by the US Armed Forces in Afghanistan is just the latest to show that a careful and forward-looking approach is needed in the development and use of digital technologies in the public sector.

To get to the heart of the matter, we can start considering the following three cases related to data processing in the field of digital public services. These cases refer to the European context, where the attention to data protection is higher and historically much more developed than in other areas, as demonstrated by the long history of Convention 108.

Case Study I: Wi-Fi tracking system [tracking risk, re-identification, data protection by design]

The Dutch SA fined the municipality of Enschede for using Wi-Fi tracking in the city centre in a way that made it possible to track shoppers and people living or working in the city centre.

Facts: Sensors placed in shopping streets to detect Wi-Fi signals from the mobile phones of passers-by. Each phone was registered separately with a unique code.

Period: 2018-2020

Sanction fee: EUR 600,000

The sensors measured how crowded streets were by counting how many phones were near the sensors at a given time. By monitoring over a longer period of time which phones were passed near the different sensors it was possible to track people. The SA found no evidence that this actually happened, but personal data and privacy were not adequately protected, and people could be tracked without this being necessary.

[*] Associate Professor of Private Law and Law & Technology, Department of Management and Production Engineering, Polytechnic of Turin, Italy.

Case Study II: Clearview AI case [legal basis, transborder data flows, proportionality]

The Swedish SA found that the Swedish Police Authority processed personal data in breach of the Swedish Criminal Data Act when using the Clearview AI image database to identify individuals.

Facts: Use of Clearview AI for biometric personal identification
Period: 2009-2020
Sanction fee: SEK 2,500,000 (about EUR 250,000)

The images were biometrically matched against a very large number of images scraped from the Internet by Clearview AI (US) to identify, among others, the target in suspected child sex offences and unknown persons in the investigation of serious organised crime. The processing operations were carried out without performing an impact assessment before starting them.

The Police Authority accessed to a large amount of personal data through the use of Clearview AI and it is unclear how long the personal data entered was processed, and how long the matching data retained. Actual damage was not demonstrated, but the potential unaddressed risk was considered sufficient for sanctions, in line with the jurisprudence of the European Court of Justice.

Case Study III: Hospital Electronic Patient Records [task allocation, accountability, security]

An investigation conducted by the Portuguese SA revealed that there was one hospital where hospital staff, psychologists, dietitians and other professionals accessed patient data through false profiles. The hospital had 985 registered doctor profiles while having only 296 doctors. In addition, doctors had unrestricted access to all patient files, regardless of the doctor’s specialty.

Facts: Illegitimate access to health data
Period: ?-2018
Sanction fee: EUR 400,000

The Portuguese SA found that the data controller allowed professionals to have indiscriminate access to EPRs and never asked the Ministry of Health shared services to adjust the access profile of hospital professionals.

Based on the brief examination of these cases, we can identify two main elements of the digital context characterising innovative public sector services, and several guiding components for a better development and deployment of these services from a human rights-oriented perspective.

As regards the context, the growing connotation of our society as a socio-technical system, where technology and human behaviour are strongly intertwined, is the first crucial aspect to considered. The second concerns the complexity and, in some cases, the obscurity of data-driven solutions, which regard the manner how these systems work but also the way they are designed by companies and AI developers.

In this scenario, five main responses should be put in place for an effective answer to potential challenges and negative impacts on individuals and society: (i) the adoption of a rights-based approach; (ii) a critical approach to technology, based on proportionality and balancing of interests; (iii) procedural rules that promote data security and accountability with regard to processed data, data flows, and actors involved (e.g. data management plans, task management ect.); (iv) risk assessment/management procedures and data protection (and human rights) by-design approach; (v) the precautionary principle as a default rule in case of uncertainty about the impact of technology innovation.

2. The role of Convention 108+

In the scenario described, pervasive datafication, complexity of data processing, cross-sectoral use of information, and predictive technologies challenge the data protection regulatory models dating from the 1970s and 1980s.

In response to these new challenges, the modernised version of Convention 108 (Convention 108+) ‘upgraded’ the framework established in 1981 by Convention 108, while maintaining its international and principles-based nature which makes it more open to enlargement than regional instruments based on national and detailed rules, such as the GDPR.

Convention 108 with its 55 ratifications and accessions is the only existing international instrument on data protection and the convergence on its principles and provisions by countries from different continents and legal cultures shows its role as a reference framework for those countries aiming to establish a coherent and robust regulatory environment on data protection.

One of the main objectives of the Convention is to put individuals in a position to know, understand and control the processing of their personal data. It refers to self-determination, personal autonomy, and the right to control one’s personal data (which stems from the right to privacy), as well as to the dignity of individuals, not to let data-driven systems to treat individuals as mere objects.

The Convention covers data processing relating to individuals, whether in the public or private sector, with the exclusion of processing carried out for purely personal or household activities.

In protecting all individuals, regardless of their nationality or residence, with respect to the processing of their personal data and in contributing to respect for human rights and fundamental freedoms (in particular the right to privacy), the Convention adopts a principles-based approach. It sets out key principles and requirements for data processing and adopts a co-regulatory approach that combines the provisions of the Convention with specific recommendations and guidelines (e.g., Guidelines on Artificial Intelligence and Data Protection).

The Convention is thus a general and flexible instrument that provides Parties with a margin of manoeuvre in implementing its principles and requirements, and offers an international framework which ensures consistency and convergence with other relevant legal frameworks. Moreover, given its open structure, any country in the world with a complying data protection legislation can accede to the Convention, which is the only existing international legal standard in this field.

Like in Convention 108, also in its modernised version, the legitimacy of data processing is based on the principles of proportionally and purpose specification, the lawfulness of processing, and the presence of a legitimate basis. Data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of any other legitimate basis laid down by law.

Other key principles, already laid down in Convention 108 – and later incorporated in all the data protection laws –, include data minimization, storage limitation and data quality (accuracy, integrity, and confidentiality). In addition to further detailing these principles, one of the main contributions of Convention 108+ relates to its focus on the accountability principle, which requires data controllers and, where applicable, data processors to take all appropriate measures to comply with their data protection obligations and to be able to demonstrate – to the competent supervisory authority – that the data processing under their control is in accordance with the law.

Another fundamental step towards effective data protection in a challenging data-driven world is the new set of provisions on risk assessment. Data controllers and, where applicable, data processors must examine the likely impact of the intended data processing on the human rights and fundamental freedoms of data subjects before such processing begins.

Based on this assessment, they will design data processing to prevent or minimise the identified risk of interference with human rights and fundamental freedoms by adopting appropriate technical and organisational measures. This by-design approach also applies to data security where the traditional focus on security measures is now combined, in Convention 108+, with a specific duty of notification regarding those data breaches that may seriously interfere with human rights and fundamental freedoms of data subjects.

In line with the original text adopted in 1981, further provisions of Convention 108+ deal with the transparency of data processing by ensuring that information about data processing and its authors is provided to data subjects. This information relates to the identity and habitual residence or establishment of the controller, the legal basis of intended processing, its purposes and the categories of personal data processed. In case of communication to third parties, information on the recipients or categories of recipients of personal data is also provided.

Data subjects must also be informed about their rights in relation to data processing, whose range has been broadened under Convention 108+. Alongside traditional access rights, new rights are granted to data subjects, strengthening the right to obtain knowledge of the reasoning underlying data processing where the results of such processing are applied to data subjects, the right to object, and the right not to be subject to a decision significantly affecting data subjects based solely on an automated data processing without their views being taken into consideration.

Like in Convention 108, greater protection is provided for special categories of data[1] due to the deeply intrusive nature of processing and the risk of discrimination which require appropriate safeguards ensured by law.

Given the level of protection provided by the Convention to individuals with regard to personal information and privacy, it is crucial not to lower these safeguards by circumventing the provisions of the Convention, in particular by transferring personal data to third countries that do not offer the same level of protection.

To this end, Convention 108+, like the original Convention, sets out specific rules for transborder data flows. Transfers to countries not party to the Convention must be based on specific requirements to ensure an appropriate level of protection.

When the law of a State or an international organisation (including applicable international treaties or agreements) does not ensure an appropriate level of protection, ad hoc or approved standardised safeguards provided by binding and enforceable legal instruments can be used. In a narrower range of cases, data transfer to third countries may also be based on data subject's consent, specific interests of the data subject, prevailing legitimate interests provided for by law, or be considered as a necessary and proportionate measure in a democratic society for freedom of expression.

These restrictions do not apply between the Parties to the Convention, because of the uniform level of protection granted by this international instrument which makes the free flow of data between them possible. There are only exceptional restrictions in case of real and serious risks that the transfer would lead to a circumvention of the provisions of the Convention or when the restriction is a consequence of binding harmonised rules of protection shared by states belonging to a regional international organisation (e.g., the GDPR, as far as EU countries are concerned).

Like in Convention 108, a crucial role in the implementation of data protection principles and safeguards is played by data protection authorities. To fulfil with their tasks (which include, *inter alia*, powers of investigations, decisions in cases of violation of data protection provisions, and standardisation of safeguards for transborder data flows), these supervisory authorities must act with full independence and impartiality in performing their duties and exercising their powers. This independence also includes an effective financial autonomy; supervisory authorities must therefore be provided with the resources necessary for the effective performance of their functions and exercise of their powers.

Given the global scenario of data processing, international co-operation between supervisory authorities is a key element for effective protection of individuals. Convention 108+ reinforces such co-operation, notably by requiring Parties to render mutual assistance, and providing the appropriate legal basis for co-operation and exchange of information for investigations and enforcement.

Finally, to foster the effective implementation of the principles of the Convention, the modernised version has adopted a follow-up mechanism which requires each party to

[1] Special categories of data include (i) genetic data; (ii) personal data relating to offences, criminal proceedings and convictions, and related security measures; (iii) biometric data uniquely identifying a person; (vi) personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life.

allow the Convention Committee to evaluate the effectiveness of the measures taken to give effect to the provisions of the Convention.

Considering the whole framework provided by the Council of Europe in the field of data protection, including a series of coordinated soft law instruments adopted over the years, and the opening of the Convention to states that are not members of the Council of Europe, Convention 108+ is the best candidates to build a global standard that can foster convergence between differing cultural and legal frameworks, and to better address the challenges of innovative data processing solutions.

3. Data protection in the context of AI-driven solutions

Artificial Intelligence (AI) systems are providing new and valuable solutions to address needs and challenges in a variety of fields and will increasingly be used in public sector decision-making processes. AI applications may represent a useful tool for decision making in particular for supporting evidence-based and inclusive policies.

As with other technological innovations, the use of AI may also have adverse consequences for individuals and society. To prevent them, the Parties to Convention 108 have adopted specific guidelines on AI and data protection to ensure that AI development and use respect the rights to privacy and data protection, thereby enhancing human rights and fundamental freedoms.

The Guidelines on artificial intelligence and data protection, adopted by the Committee of the Convention for the Protection of Individuals with regards to Processing of Personal Data (Convention 108) on 25 January 2019, provide a set of baseline measures that governments, AI developers, manufacturers, and service providers should follow to ensure that AI applications do not undermine the human dignity and the human rights and fundamental freedoms of every individual, in particular with regard to the right to data protection.

These Guidelines are divided into three main building blocks that shows their concrete and operational approach compared to the theoretical and abstract nature of several guidelines on AI: (i) general guidance; (ii) guidance for developers, manufacturers and service providers; (iii) guidance for legislators and policy makers.

In applying the principles of Convention 108+ to AI, the Committee of Convention 108 has focused on avoiding and mitigating the potential risks of AI related to individuals. In line with the previously adopted Guidelines on Big Data (2017), the Committee suggests a broader view of possible outcomes of data processing which considers not only human rights and fundamental freedoms, but also the functioning of democracies and social and ethical values. AI applications should therefore allow meaningful control by data subjects over data processing and its effects on individuals and on society.

As regards AI developers, manufacturers and service providers, they should adopt a values-oriented approach in the design of their products and services, in a manner consistent with Convention 108+ and assess the possible adverse consequences of AI applications on human rights and fundamental freedoms. In considering these consequences, they should adopt a precautionary approach based on appropriate risk prevention and mitigation measures.

A by-design approach focused on human rights and avoiding potential bias is presented as crucial in the development and use of AI, as is the assessment of the quality, nature, origin and amount of personal data used, including the reduction of unnecessary, redundant or marginal data during the development, and training phases.

The Guidelines also highlight the need to counter the risk of adverse impacts on individuals and society due to de-contextualised data and de-contextualised algorithmic models, and the role that independent multidisciplinary committees of experts, as well as independent academic institutions, can play in contributing to the design of human rights-based, ethically, and socially oriented AI applications.

Participatory forms of risk assessment, based on the active engagement of the individuals and groups potentially affected by AI applications, are encouraged by the Guidelines, as well as the adoption of forms of vigilance that promote the accountability of all relevant stakeholders throughout the entire lifecycle of these applications to ensure compliance with data protection and human rights principles (algorithmic vigilance).

Regarding end-users' rights, AI developers, manufacturers and service providers are encouraged to design their products and services in a way that safeguards users' freedom of choice regarding the use of AI, by providing viable alternatives to AI applications. In addition, data subjects should be informed if they interact with an AI application and have the right to obtain information about the reasoning underlying AI data processing operations applied to them, including the consequences of such reasoning.

In the last section on guidance for legislators and policy makers, the Committee of Convention 108 emphasises the importance of the principle of accountability, the adoption of risk assessment procedures and the application of other appropriate measures, such as codes of conduct and certification mechanisms, to increase trust in AI products and services.

The public sector, though procurement procedures, can play an important role in imposing on AI developers, manufacturers, and service providers these duties of transparency, prior assessment of the impact of data processing on human rights and fundamental freedoms, and vigilance on the potential adverse effects and consequences of AI applications.

When adopting AI solutions, it is also important that the overreliance on responses provided by AI is countered by preserving the role of human intervention in decision-making processes and the freedom of human decision-makers not to rely on the outcome of recommendations provided by AI.

Finally, when AI applications may significantly impact on human rights and fundamental freedoms, data protection authorities can play an important role in prior consultations and in promoting the cooperation with other bodies having competence in AI-related matters (e.g., consumer protection, competition, anti-discrimination, and media regulatory authorities). In addition, these authorities can promote a more inclusive debate on AI by ensuring that individuals, groups, and other stakeholders are informed and actively involved in the evaluation of AI solutions that could potentially affect them.

4. Digital innovation and human rights in the public sector

Based on the cases outlined in the scenario description (Section 1) and the considerations regarding the impact of digital innovation on individual rights (Sections 2 and 3), namely the right to the protection of personal information and the right to privacy, the public sector can play a crucial role in promoting a human rights-oriented use of innovative digital technologies, including AI.

In this regard, the analysis of the case studies and the regulatory framework for data processing make it possible to outline some key insights for future regulatory policies for digital administration.

The first element to consider is the socio-technical nature of those digital solutions, which is even more evident in the case of AI applications. Digital services are no longer used to optimise documental flows or back-office tasks but to analyse society, target groups and individuals, providing context-specific personalised services and supporting (or making) public sector decisions.

Based on this scenario, a second takeaway concerns the importance of not following a data-driven approach inspired by techno-solutionism, underestimating the diverse impacts that alternative technology solutions may have on individuals and society, as well as the values that technological artefacts necessarily embody. In this sense, the experience of contract tracing applications during the Covid-19 pandemic, the extensive use of vaccine passports, and other forms of social and individual monitoring have raised several issues in terms of proportionality and impact on human rights and freedoms.

This urges a human rights-centred approach to technology development and adoption, which considers all the potential effects of digital services and avoids or minimises their negative impacts on human rights and freedoms.

Awareness of both the technology and its impact is therefore needed, based on a critical approach that takes into account the proportionality of the planned proposals and the related balancing of interests.

With regard to the use of personal data, this entails a preliminary analysis of the categories of data processed, data flows, and actors involved in data processing, followed by an assessment and management of potential risks to the data protection and human rights in general. This requires a focus on these issues from the outset of product/service design and the adoption of appropriate by-design solutions to create digital infrastructure and services oriented towards the protection of individual rights.

In this context, it is crucial for public administration to set up a proper task allocation, with key figures dedicated to data protection, and to oversee the most impactful projects, as well as to put in place sector-specific training initiatives, which play an active role in raising awareness and strengthening human rights-centred digital skills among public servants.

Alongside this attention to internal organisation, an important role can also be played by supervisory authorities, in particular data protection authorities, through communication campaigns to increase privacy awareness and knowledge of their rights by data subjects, but also by putting in place public sector support and training initiatives. This proactive communication and support approach would be more effective in the long run than a strategy centred simply on sanctions and enforcement.

In addition, effective engagement of the key stakeholders in public sector initiatives and programmes led by supervisory authorities could contribute to a better understanding of the main issues to be addressed by decision-makers. This will also facilitate the implementation of legal provisions and the adoption of best practices, including opening up the public administration to a more inclusive and transparent action.

Finally, special attention should be paid to partnerships and contracts with foreign service provides, assessing the level of protection they offer to personal data and human rights. To this end, as discussed in relation to Convention 108+, a key role is played by the control over transborder data flows and the level of protection provided by third parties in data processing.

States can intervene directly by setting specific requirements for transborder data transfers, but asymmetric relationships among states may reduce their margin of manoeuvre, especially when they are not parties to international conventions, such as Convention 108+, which can provide them with a sound and internationally recognised systems of rules. In the absence of such safeguards provided by law, public administration can adopt solutions on a case-by-case basis, relying on contractual, organisational and technical measures, taking into account that while the former (e.g. audits, inspections, transparency policies, accountability, and standards) may be of help in most cases, technical solutions (e.g. encryption, strong pseudonymisation) should be implemented when service providers are based in countries that grant extensive power of inspection to government agencies.