**COUNCIL OF EUROPE**

**CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (CETS NO. 108) AND AMENDING PROTOCOLS**

*Federica Cristani\**

# 1. Introduction and short overview of the instrument

The Council of Europe´s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108)[[1]](#footnote-1) was open for signature in 1981 and it was the first legally binding international instrument in the field of data protection. To date, it counts 55 parties and 32 observers.[[2]](#footnote-2) As affirmed in article 1, “[t]he purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him”. The Convention provides obligations for the parties to apply the principles regarding the processing of personal data in their domestic legislation.

Chapter II of the Convention lays down the basic principles for data protection, including: the duties of the state parties (Article 4), quality of data (Article 5), definition of special categories of data (Article 6), as well as provision on data security (Article 7), additional safeguards for the data subject (Article 8), exceptions and restrictions (Article 9), sanctions and remedies (Article 10) and the conditions for extended protection (Article 11). Chapter III deals with transborder flows of personal data and domestic law (Article 12), while Chapter IV is dedicated to the question of mutual assistance, which includes provisions on the co-operation between the state parties (Article 13), assistance to data subjects resident abroad (Article 14), safeguards concerning assistance rendered by designated authorities (Article 15), refusal of requests for assistance (Article 16), costs and procedures of assistance (Article 17).

Chapter V foresees the establishment of a Consultative Committee, which “a. may make proposals with a view to facilitating or improving the application of the Convention; b. may make proposals for amendment of this Convention […]; c. shall formulate its opinion on any proposal for amendment of this Convention […]; d. may, at the request of a Party, express an opinion on any question concerning the application of this Convention” (Article 19). The Consultative Committee is composed of representatives of Parties to the Convention complemented by observers that include non-member States represented by their governments or data protection authorities, international organisations and non-governmental organisations (Article 18). The Consultative Committee, which includes 70-80 members and observers, offers a unique forum for discussions and deliberations concerning the rights to privacy and data protection at multilateral level.[[3]](#footnote-3)

In 2001, an Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181)[[4]](#footnote-4) was opened for signatures. Indeed, the increased exchanges of personal data across national borders made it necessary to update the Convention. The Additional Protocol, in particular, requires state parties to set up supervisory authorities, which would operate in complete independence.

Most recently, another Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223)[[5]](#footnote-5) was opened for signatures in 2018 with the aim to modernize Convention 108 with respect to the challenges to privacy resulting from the use of new information and communication technologies. Among the innovations included in the Protocol, we can mention: the introduction of stronger requirements regarding the proportionality and data minimization principles; the extension of the types of sensitive data, which will now include genetic and biometric data, trade union membership and ethnic origin; stronger accountability of data controllers; the introduction of the requirement that the “privacy by design” principle is applied; application of the data protection principles to all processing activities, including for national security reasons; introduction of a clear regime of transborder data flows; and reinforced powers and independence of the data protection authorities and enhancing legal basis for international cooperation.

# 2. Human rights addressed

**Right to privacy** is guaranteed at the international level by article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights.

Convention 108+[[6]](#footnote-6) lays down in Chapter II the basic principles for the protection of personal data. In particular, article 5 (Legitimacy of data processing and quality of data) specifies that

[d]ata processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.

[…] Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law.

In particular, as specified further in paragraph 4 of article 5,

[p]ersonal data undergoing processing shall be:

a. processed fairly and in a transparent manner;

b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date;

e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

Article 6 of the Convention (Special categories of data) lays down specific safeguards for some categories of data, namely "genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data uniquely identifying a person; 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“. In particular, as specified in paragraph 2 of article 6, "[s]uch safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination".

It is also worth mentioning Article 11 (Exceptions and restrictions) of Convention 108+, which provides a set of conditions and safeguards to be put in place for data processing carried out for a rather restricted list of purposes (namely, "the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offenses and the execution of criminal penalties, and other essential objectives of general public interest; and […] the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression“) and which aims at ensuring that any interferences is permissible and deemed as lawful in a democratic society. The Committee of Convention 108 is currently working on a Guidance Note on art 11 to suggest more clarity and details of the conditions and safeguards.[[7]](#footnote-7)

# 3. Challenges in implementation: a focus on the implementation of the Convention during the COVID-19 pandemic

The outbreak of the COVID-19 pandemic has opened up to the use of different technologies by states around the world; indeed, among the different legal, political, and public health responses to COVID-19, countries were employing technological instruments to track the spread of the pandemic within their territories[[8]](#footnote-8) and monitor the citizens’ abidance with governmental measures such as quarantine.[[9]](#footnote-9)

Digital technologies that were employed include mobile and biometric applications; in particular, those based on geolocation provide data about the geographical spread of the virus, as in the case of the call data records (CDRs), namely the data that are elaborated by telecommunication service providers and are based on telephone calls, which enable the tracing of the movements of people on both a temporal and geographical scale. In this respect, the Robert-Koch Institute in Germany used anonymised movement flows data collected by the German telecommunications provider Deutsche Telekom,[[10]](#footnote-10) while in Italy, an aggregated and anonymous heat map –based on anonymised datasets– for the Lombardy region to better understand population movements was produced by Vodafone.[[11]](#footnote-11)

Alongside the data that can be collected by telecommunication service providers, governments launched new mobile applications for tracing the spread of COVID-19.[[12]](#footnote-12) Singapore, for example, used the TraceTogether App, developed by the Government Technology Agency of Singapore in collaboration with the Ministry of Health, which has also served as a model for similar contact tracing apps in other countries.[[13]](#footnote-13) Also in Europe, several states released tracking mobile applications.[[14]](#footnote-14)

While these technologies can help governmental authorities in monitoring the spread of the virus and fulfill their obligations to protect the rights to health and life of their citizens, they bring along also a number of concerns: in particular, legal concerns arise about the collection and use of data and the respect of the right to privacy of the users of the mobile applications. Indeed, a tracking app can collect a broad range of personal data; in some cases, apps continue to run in the background even when the device is not in use, while other apps can exchange information with other devices. Moreover, a number of countries implemented mobile applications that use facial recognition or other biometrics smartphone apps, such as in Poland, China and Russia, which may raise additional concerns, e.g. when facial recognition is based on race or ethnic origin.

Against this background, the Council of Europe has been quite active in addressing such concerns and providing guidance for states in this respect. On 30 March 2020, the Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe issued their first Joint-Statement on the right to data protection in the context of the COVID-19 pandemic, which re-affirmed that “States have to address the threat resulting from the COVID-19 pandemic in respect of democracy, rule of law and human rights, including the rights to privacy and data protection”.[[15]](#footnote-15)

On 28 April 2020, the Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe issued their second Joint Statement on Digital Contact Tracing, recalling that “large-scale personal data processing can only be performed when, on the basis of scientific evidence, the potential public health benefits of such digital epidemic surveillance (e.g. contact tracking), including their accuracy, override the benefits of other alternative solutions which would be less intrusive”.[[16]](#footnote-16) The Joint Statement establishes conditions of acceptability of a digital contact tracing system, specifying that “the acceptability of a digital contact tracing system clearly depends on the trust that such a system can inspire, and deliver. […] Achieving broad acceptability can thus be supported by implementing a trustworthy system, which is not imposed upon people but used on a voluntary basis instead. This also means that there should be no negative consequences imposed for not participating in the system”.

Later, on 12 October 2020, the Data Protection Unit of the Council of Europepublishedthe report “*Digital solutions to fight COVID-19*”,[[17]](#footnote-17) which offers an overview on how personal data have been processed in the 55 State Parties of Convention 108+ during the COVID-19 pandemic. The reports shed lights on some practices that have been followed by Parties, such as the use of privacy impact assessment and privacy by design principles in developing digital solutions to support public health measures. As the report highlights, “[t]he role of international fora such as the Council of Europe is essential in recalling the path to take, issuing recommendations and guidance, enabling exchange of information and best practices. […] The manner in which the health crisis has been addressed prompts a reaffirmation of the resilience of the data protection principles as a key component of the effective functioning of our democracies”.

# 4. Similar initiatives elsewhere

Since its adoption in 1981, Convention 108 has influenced various regional and national privacy regulations. At the regional level, we can mention the work on privacy and data protection carried on by the European Union and the African Union. The European Union´s Charter of Fundamental Rights stipulates that EU citizens have the right to protection of their personal data.[[18]](#footnote-18) At the same time, the European Union has issued several directives and regulations on data protection, like the General Data Protection Regulation (GDPR).[[19]](#footnote-19) On the other hand, the African Union adopted the AU Convention on Cyber Security and Personal Data Protection (known as Malabo Convention) in June 2014 -[[20]](#footnote-20) which entered into force on 8 June 2023.[[21]](#footnote-21) Convention 108 has also served as the foundation for international data protection law in several countries (as recalled by the Draft explanatory report to the Convention for the protection of individuals with regard to automatic processing of personal data [ETS No. 108] prepared in 2016).[[22]](#footnote-22)

# 5. Recommendations

As the only legally binding international instrument with worldwide scope on data protection, Convention 108 provides a unique international platform for cooperation. Besides the member states of the Council of Europe, also Argentina, Cap Verde, Mauritius, Mexico, Senegal, Uruguay and Tunisia have become parties to the Convention. The modernised treaty is not yet in force; its ratification by as many states as possible should instead be encouraged, in order to ensure that its data protection principles can be efficiently adapted to new technologies worldwide.

1. \* Federica Cristani is Head of the Centre for International Law, Institute of International Relations, Prague, and Visiting Senior Researcher at the Arctic Centre of the University of Lapland. E-mail: [cristani@iir.cz](mailto:cristani@iir.cz).

   Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), opened for signatures on 28 January 1981, <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108>. [↑](#footnote-ref-1)
2. For the full lists of siggnatures and ratification, see the official webpage: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>. [↑](#footnote-ref-2)
3. For the current list of members and more details on its activities, see the official webpage at <https://www.coe.int/en/web/data-protection/consultative-committee-tpd#:~:text=Established%20by%20Convention%20108%2C%20the,organisations%20and%20non%2Dgovernmental%20organisations>.. [↑](#footnote-ref-3)
4. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181), opened for signatures on 8 Noevmber 2001, <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=181>. [↑](#footnote-ref-4)
5. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), opened for signature on 10 October 2018, <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=223>. [↑](#footnote-ref-5)
6. The Consolidated version of the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, updated to Protocol CETS No. 223, is available at <https://www.coe.int/en/web/data-protection/convention108-and-protocol>. [↑](#footnote-ref-6)
7. The Working Draft Legal Instrument on Government-Led Surveillance and Oversight Including the Explanatory Memorandum for article 11 of Convention 108+, issued on 6 October 2022, is available at <https://rm.coe.int/t-pd-2022-5-modernised-convention-108-article-11-guidance-document-en/1680a86970>. [↑](#footnote-ref-7)
8. On the use of technologies in tracking the spread of COVID-19, see Privacy International, *Apps and Covid-19* (2020), <https://privacyinternational.org/examples/apps-and-covid-19> and Lorna McGregor, "Contact-tracing Apps and Human Rights”, EJIL: Talk! Blog (30 April 2020), <https://www.ejiltalk.org/contact-tracing-apps-and-human-rights/>. [↑](#footnote-ref-8)
9. OECD, “Tracking and tracing COVID:Protecting privacy and data while using apps and biometrics” *OECD Policy Responses to Coronavirus (Covid-19)* (23 April 2020), <https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/>. [↑](#footnote-ref-9)
10. Stephan Broszio, “Corona prediction: Telekom supports RKI” *Telekom* (18 March 2020), <https://www.telekom.com/en/company/details/corona-prediction-telekom-supports-rki-597114>. [↑](#footnote-ref-10)
11. Vodafone, *Vodafone launches five-point plan to help counter the impacts of the COVID-19 outbreak* (18 March 2020), <https://www.vodafone.com/about-vodafone/where-we-operate/roaming-services/vodafones-5-point-plan-help-counter-impacts-covid-19-outbreak> and Privacy International, *Vodafone produces anonymous heat map to help Lombardy understand population movements* (18 March 2020), <https://privacyinternational.org/examples/3428/vodafone-produces-anonymous-heat-map-help-lombardy-understand-population-movements>. [↑](#footnote-ref-11)
12. Indeed, contact-tracing is a common technique in public health surveillance. See World Health Organizazion, C*ontact tracing and quarantine in the context of COVID-19: interim guidance* (6 July 2022), <https://www.who.int/publications/i/item/WHO-2019-nCoV-Contact_tracing_and_quarantine-2022.1>. [↑](#footnote-ref-12)
13. See the official website at <https://www.tracetogether.gov.sg>. [↑](#footnote-ref-13)
14. See European Commission, *Mobile contact tracing apps in EU Member States* (2023), <https://commission.europa.eu/strategy-and-policy/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en>. [↑](#footnote-ref-14)
15. Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe (30 March 2020), <https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter>. [↑](#footnote-ref-15)
16. Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe (28 April 2020), <https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7>. [↑](#footnote-ref-16)
17. Data Protection Unit of the Council of Europe, *Digital Solutions to Fight Covid-19. 2020 Data Protection Report* (October 2020), <https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c>. [↑](#footnote-ref-17)
18. Article 8 of the Charter of Fundamental Rights of the European Union, declared in 2000, and entered into force since December 2009 along with the Treaty of Lisbon. The text is available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>. [↑](#footnote-ref-18)
19. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [↑](#footnote-ref-19)
20. African Union Convention on Cyber Security and Personal Data Protection, adopted on 27 June 2014, available at <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>. [↑](#footnote-ref-20)
21. After Mauritania’s ratification on 9 May 2023. According to article 36, the Convention could enter into force thirty days after the date of receipt of the fifteenth instrument of ratification. [↑](#footnote-ref-21)
22. The Draft explanatory report is available at <https://rm.coe.int/convention-for-the-protection-of-individuals-with-regard-to-automatic-/16806b6ec2>. [↑](#footnote-ref-22)