COMMITTEE
OF MINISTERS
COMITÉ
DES MINISTRES

COUNCIL OF EUROPE
1949 - 2024
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES Recommendations **CM/Rec(2024)5** 9 October 2024

Recommendation CM/Rec(2024)5 of the Committee of Ministers to member States regarding the ethical and organisational aspects of the use of artificial intelligence and related digital technologies by prison and probation services

(Adopted by the Committee of Ministers on 9 October 2024
at the 1509th meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe (ETS No.1),

Having regard to the European Convention on Human Rights (ETS No. 5) and the case law of the European Court of Human Rights;

Having regard to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), as amended by its Protocol (CETS No. 223, "Convention108+"); and in particular: the Guidelines on artificial intelligence and data protection; the Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, the Guidelines on facial recognition and the Guidelines on national digital identity;

Having regard also to the European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (ETS No. 126) and to the work carried out by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment, and in particular the standards it has developed in its general reports;

Having further regard to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225);

Endorsing the standards contained in the relevant recommendations of the Committee of Ministers of the Council of Europe to member States and in particular in recommendations: Rec(2006)2-rev (revised and amended by the Committee of Ministers on 1 July 2020) on the European Prison Rules; CM/Rec(2008)11 on the European Rules for juvenile offenders subject to sanctions or measures; CM/Rec(2010)1 on the Council of Europe Probation Rules; CM/Rec(2012)5 on the European Code of Ethics for Prison Staff; CM/Rec(2014)3 concerning dangerous offenders; CM/Rec(2014)4 on electronic monitoring; CM/Rec(2017)3 on the European Rules on community sanctions and measures; CM/Rec(2020)1 on the human rights impacts of algorithmic systems and CM/Rec(2023)2 on rights, services and support for victims of crime;

Taking also into consideration Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling;

Drawing attention also to the European Union General Data Protection Regulation 2016/679 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 and the European Union Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA as well as to the Organisation for Economic Co-operation Development's Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449);

Taking into account the specific conditions under which prison and probation services operate and their role in the execution of penal sanctions and measures, which are among the strongest manifestations of public powers imposed on individuals and which may interfere deeply with their human dignity, human rights and privacy, including the collection and processing of personal data;

Recognising in this respect that the rapid development and use of digital technologies, as well as of artificial intelligence (AI), in all spheres of social life can bring a number of positive changes in our societies but also raise a number of ethical concerns regarding human rights, respect for private life and data protection;

Noting that the collection of biometric data and the use of algorithms by the criminal justice system are advancing at a great pace in Europe and are gaining more importance at all the stages and in every area of the criminal justice system;

Noting also that digital and AI literacy needs to be enhanced among key actors in the criminal justice system and urgent measures need to be taken to prepare them to make efficient and ethical use of AI and related digital technologies in their everyday work to the benefit of other individuals using these technologies and those subject to them;

Drawing attention to the need for these tools to be commissioned for design, development and maintenance to carefully selected and vetted private companies which work in close co-operation with the prison and probation services. These companies should be made aware that high ethical standards and principles and strict professional rules should be respected, and that the main objectives should be community safety and rehabilitating offenders, not making profits;

Emphasising therefore that it is critical to develop rapidly, to regularly review and, if necessary, revise the principles and standards which should guide the prison and probation services of its member States when using AI and related digital technologies in order to preserve high ethical and professional standards;

Further stressing that AI and related digital technologies should be used not only for safety and security purposes but also for the social inclusion of persons in conflict with the law and that their reintegration should remain central. This use should not undermine the human-centred approach and should avoid contributing to discrimination and economic and social inequalities,

Recommends that governments of member States:

- be guided in their legislation, criminal policy and practice by the principles and rules contained in the appendix to this recommendation;

- ensure that this recommendation and its explanatory memorandum are translated and disseminated as widely as possible and, more specifically, among judicial authorities, prosecution, police, prison, probation and juvenile justice services, as well as among private companies which design and provide AI and related digital technologies in the framework of the criminal justice system.

Appendix to Recommendation CM/Rec(2024)5

I. General provisions

a. This recommendation seeks to provide guidance related to the ethical and organisational aspects of the use of artificial intelligence (AI) and related digital technologies in prisons and by probation services. AI is a rapidly developing area and therefore public authorities are invited to adopt and respect additional standards related to the protection of the rights and freedoms of the users of AI, including those affected by its use.

b. The public authorities in charge of prison and probation services should remain fully responsible for ensuring respect for the principles and standards contained in this recommendation. They should also ensure that the private companies which design, develop, provide, use and decommission such technologies follow the same ethical and organisational principles and standards as stated in this recommendation.

c. The juvenile justice services should make use of these rules in a manner adapted to the specific needs of juveniles.

d. AI and related digital technologies should be used legitimately and proportionately when and if they:

- contribute to the rehabilitation and reintegration of offenders;
- do not replace prison and probation staff but assist them in their everyday work;
- help the criminal justice system, the execution of penal sanctions and measures and the reduction of recidivism.

II. Definitions

For the purposes of this recommendation, the following definitions are used:

- “artificial intelligence (AI)” means a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment;

- “related digital technologies” is a generic term that refers to all electronic devices, automatic systems and technological resources that generate, process or store information and data which are being used by AI.

III. Basic principles

1. When designing, developing, providing, using and decommissioning AI and related digital technologies, respect for human rights and the dignity of all persons affected by this use should be ensured (principle of respect for human dignity and fundamental rights).

2. All processes related to the design, development, provision, use and decommissioning of AI and related digital technologies to be used by the prison and probation services and the private companies acting on their behalf should be in conformity with the relevant international standards and with national law. Liability for any unlawful harm caused by the use of AI and related digital technologies should be ensured (principle of legality, legal certainty and liability).

3. Biases should be avoided when designing, developing, providing, using and decommissioning AI and related digital technologies. Measures should be taken to ensure equality and to prevent or resolve the creation or intensification of any discrimination or inequality between individuals or groups of individuals (principle of equality and non-discrimination).

4. AI and related digital technologies should be used only in a manner that implies the least negative impact on human rights and if their intended use and intensity correspond to the purpose and the expected results. In addition, this should be done only if strictly necessary (principle of proportionality, efficacy and necessity of AI).

5. The process of designing, developing, providing, using and decommissioning AI and related digital technologies should be transparent to public scrutiny and monitored on a regular basis, and the logic behind and the outcomes of their use should be explainable at a reasonable level (principle of good governance, transparency, traceability and explicability).

6. When a decision based on the use of AI and related technologies affects the human rights of potential users, a procedure should be put in place for a human review and an effective complaint mechanism in accordance with national law (principle of the right to a human review of decisions).

7. Reliable and accurate AI and related digital technologies should be based on certified sources, tangible data and validated scientific methods and values. Data should be accurate and the samples sufficiently representative of the key characteristics of the general population and minority groups, including the target groups that might be affected. The design and use of AI and related digital technologies should be done in a secure and audited technological environment in order to ensure the safety and security of these tools, their users and those affected by their use (principle of quality, trustworthiness and security).

8. AI and related digital technologies should be used in a manner which preserves and promotes positive and beneficial human relations between staff and offenders, as these relations are instrumental in changing behaviour and in ensuring social reintegration (principle of human-centred use of AI and related digital technologies).

9. The basics of AI and related digital technologies, including how they should be used and for what purpose and the ethical rules to be respected, should be made understandable to the users (principle of AI and digital literacy).

IV. Data protection and privacy

10. Offenders continue to enjoy their fundamental rights and freedoms, including the right to respect for private life and the right to data protection, when AI and related digital technologies are used. Limitations to these rights and freedoms should only be allowed when they are in accordance with law, respect the essence of fundamental rights and freedoms, pursue a legitimate aim, are necessary in a democratic society and are proportionate.

11. All key actors, whether public or private, participating in the design, development, provision, use and decommissioning of AI and related digital technologies should comply with data protection law, be transparent in relation to the individuals concerned and be able to demonstrate that the processing of data under their control complies with data protection principles and obligations.

12. Data should be stored in a form that allows a personal identification for no longer than is strictly necessary to fulfil the purposes for which it was initially collected. Data controllers should adopt security measures to ensure the integrity and confidentiality of the stored data, preventing accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.

13. Only the amount and type of personal data which are strictly necessary to fulfil a specific task should be collected, stored, transmitted or otherwise processed. Such personal data should only be further processed for the purpose for which they were originally collected. Wherever possible, anonymised data should be used instead of personally identifiable data.

14. The collection and processing of special categories of personal data should only be allowed where it is strictly necessary and appropriate, and additional safeguards are enshrined in law. AI and related digital technologies that are based on special categories of data, such as biometric data, should be used in controlled environments to avoid false positives and undifferentiated data collection.

V. Use of AI and related digital technologies

A. Use for the purpose of safety, security and good order

15. The use of AI and related digital technologies for maintaining safety, security and good order should also allow for better risk and crisis management. Their use should be strictly necessary, proportionate to the purpose and should avoid any negative effects on the privacy and well-being of offenders and staff. Under no circumstances should the use of AI and related digital technologies cause intentional physical or mental harm or suffering to a person.

16. Prison and probation services should be consulted in order to identify and evaluate the needs regarding the assistance of staff through AI and related digital technologies in the execution of tasks related to safety, security and good order. The purpose should be to design and use well-adapted AI and related digital technologies, so that staff can retrain to improve their professional development related to safety, security and good order, which should contribute to the social reintegration of offenders.

17. The use of AI in electronic monitoring, including biometric recognition technologies, should be proportionate to the purpose and used only when strictly necessary. It should be carried out under regular human control and should be human centred. It should be oriented to favour the reintegration of offenders and should be respectful of all the principles and guarantees associated with the use of electronic monitoring and of this recommendation.

B. Use for offender management, risk assessment, rehabilitation and reintegration

18. AI and related digital technologies can be beneficial for facilitating offender management. They should be used to manage offenders’ files and particular cases and to generate automatic alerts in cases of non-compliance if this improves monitoring and decision taking. The final responsibility for this remains with the professionals. The human-centred approach should remain a key element in decision taking.

19. When developing AI and related digital technologies in order to increase the accuracy and objectivity of risk assessment, the challenges of algorithmic biases and quality and representativeness of data should be addressed. Sensitivity to all kinds of diversity, including to gender perspective and multiculturalism, should inform the design and use of risk assessment tools in order to avoid any discrimination.

20. The results of risk assessment should be used only for risk management. The decisions deriving from the risk assessment should not be automated but should be taken by appropriately designated professionals.

21. The rehabilitation and reintegration of offenders, as well as their social contacts, may be facilitated by the use of AI and related digital technologies. When such tools are used for the personalisation of treatment and reintegration plans, this should be done with care to avoid biases. The use of such tools should not replace regular face-to-face human contact between professionals and the offenders, including, where necessary, the work with their families and children.

22. AI and related digital technology tools can be used to facilitate automated and remote medical diagnosis and follow-up medical treatment in case of need, but this should not replace face-to-face professional care and treatment.

23. While AI and related digital technologies can be easily used for managing appointments and interventions (including appointments with healthcare professionals, lawyers, social workers and any other professionals), this should be done with care. Such use should facilitate, and not impede or replace entirely, face-to-face human contact and meetings of offenders with their family, professionals and relevant services.

C. The use of AI and related digital technologies for staff selection, management, training and development

24. AI and related digital technologies in the selection, management, training and development of staff should be used to optimise human and managerial capacities and processes. This use should also be focused on supporting the staff's professional development.

25. AI and related digital technologies should assist managers in predicting future organisational capacity, including detecting especially problematic areas in staff resourcing. Managerial decisions taken in this respect should not violate staff members' rights or lead to discrimination or unfairness.

26. A person should have the right to be informed of the reasons for decisions related to their selection, recruitment and professional development, taken on the basis of AI and related digital technologies, and should have the right to request their human review.

VI. Research, development, evaluation and regular revision

27. The design and development of, as well as research in, AI and related digital technologies should be sufficiently well funded and supported. These activities should be carried out with due consideration of data protection rules, with anonymised data published, and should help develop further the proper and efficient use of AI and related digital technologies and prevent potential negative effects.

28. AI and related digital technologies and their use should be evaluated at regular intervals by independent and competent evaluators concerning their performance, their intended and unintended outcomes and the need for adaptations. The initial funding should include or take into account the follow-up costs for implementation and evaluation.

29. Procedures and resources should be in place to regularly monitor, identify, assess, prevent and mitigate possible risks and adverse effects resulting from the design, development and use of AI and related digital technologies by the prison and probation services.

30. This recommendation should be reviewed regularly and revised accordingly in order to continue working to protect the human rights and fundamental freedoms of its users and the safety and security of our societies.