

Management of the IT infrastructure of the courts

- Superior Council of Magistracy-

This point of view on the management of the IT infrastructure of the courts, as described in the national contribution, is not only of the Superior Council of Magistracy, but was expressed already in 2021 by the Consultative Council of European Judges (CCJE) in Opinion No 24/2021, which was also reiterated when Opinion No 26/2023 was adopted. Thus, in Opinion No 24/2021, on the evolution of Councils for the Judiciary and their role in independent and impartial judicial systems, the CCJE stressed “the growing importance of information technology for the future of the judiciary and recommended that, where it exists, Councils for the Judiciary should have a role in this area in order to adequately protect the independence of the judiciary and ensure the quality of judges’ work in the future”^[1].

Furthermore, in Opinion No 26/2023, the CCJE emphasised the idea that ‘effective data security and data protection measures require effective and independent monitoring of the technology used by the judicial authority, as is generally the case in society. Such supervision could pose a significant risk to judicial independence if it were carried out by an executive or regulatory body, such as a national data protection supervisory authority, and not by a body of the judiciary’^[2].

The problem encountered by the Council with regard to the centralisation of databases has also come to the attention of the European Network of Councils for the Judiciary (ENCJ). In this respect, the ENCJ Executive Board adopted on 15.11.2024 **a statement on the involvement of the Councils for the Judiciary in judicial IT governance (annexed), in which it essentially stressed that** “within their mandate, the Councils for the Judiciary should have decision-making power both in the management of judicial databases (in terms of access to case data and in terms of their duties with regard to the protection of personal data) and in terms of applications used within the judiciary.

The Consultative Council of European Judges also discussed this issue at its 25th plenary meeting of the Consultative Council of European Judges (CCJE) on 4-6 December 2024.

^[1] Opinion of the CCJE No 24 (2021):

Evolution of judicial councils and their role in independent and impartial judicial systems, paragraph (24)
<https://rm.coe.int/opinion-no-24-2021-of-the-ccje-romanian/1680a5e7ca>

^[2] Opinion of the CCJE No 26 (2023): By putting forward: use of assistance technology in the justice system, paragraph (57) <https://rm.coe.int/ccje-opinion-no-26-2023-romanian/1680b1329d>

Therefore, the IT reform processes of the judiciary should be carried out with the agreement of the Councils for the Judiciary, within their mandate and in line with their role as guarantors of the independence of the judiciary.”

In this context, the position of the Superior Council of Magistracy was that the centralization process can be done even on a server purchased by the Ministry of Justice within the projects financed by the NRRP, but the data itself must be hosted in a separate domaine of courts, where the sole data administrator is an entity in the judicial system (similar to the solution agreed in the case of prosecutor's offices), preferably the Superior Council of Magistracy, which has an integrated perspective on the needs of the system. Although this solution can be implemented from a technical point of view, the Ministry of Justice did not approve this variant, arguing that under the NRRP it was established that the centralisation and taking over of the management of all data in the judicial system should be carried out at the level of the Ministry.

Although the Council cannot make its own assessment of this statement, as it does not have at its disposal the relevant data for the approval of the NRRPs by the European Commission, we consider that a financial instrument intended to support Member States, including for strengthening the rule of law, cannot lead, through the implementation of the projects, precisely to its weakening.

We therefore believe that, if such a measure has been approved by the European Commission, it would be appropriate to reconsider it, in order to establish in concrete terms the purpose and effects with regard to the independence of the justice system, which may not have been sufficiently explained.

Consequently, even in this hypothesis mentioned above, there may be mechanisms for re-establishing the facts in the projects, with the support of the European Commission, as has been the case before. We consider that we would find ourselves in a situation where such a rethinking of the competences with regard to the management of the databases of the judiciary is imperatively necessary, given that, otherwise, the premises are created for affecting the independence of the judiciary and infringement of the principle of separation of powers.

Details of the steps taken:

1. In the context in which the Ministry of Justice has started a process of enrollment of all computers in the courts, including the servers containing the databases with decisions and documents submitted by the parties (cases in electronical format), and of the judges' accounts in the just.ro domain, on **22.08.2024**, the Superior Council of Magistracy analyzed and found vulnerabilities generated by the process of enrolling court equipment in a centralized system, administered from outside the judicial authority.
2. This undertake, if completed, will give the Ministry of Justice (part of the executive power) the possibility to access any document in any case, as well as the contents of any computer of any judge or clerk in the judiciary, without a real possibility on the part of the courts or of the Superior Council of Magistracy, to prevent such access or to detect it (after it has occurred). Essentially, although security policies can be instituted, they are

under the control of the Ministry of Justice, in its capacity as manager and administrator of the system, so that, theoretically, they can be easily changed by the Ministry without the possibility of opposition or knowledge of these changes. In any case, the audit would also be done by the ministry, so that, if there would be a suspicion of unauthorized access, the Council would have no means to directly audit such a suspicion, but could only ask the ministry, and the ministry would make that verification and provide the answer.

3. Thus, until this unilateral decision to centralize the entire IT infrastructure of the courts at the level of the Ministry of Justice, there was no similar situation that would create the possibility of unrestricted access to information from cases by an institution outside the judiciary. On the contrary, prior to this approach, the information in the ECRIS (electronic file management system) information systems were stored in a decentralized architecture, with separate databases for each court. Also, the equipment within the courts is, in some situations, centrally organized, but the centralization is carried out at the level of the court or higher court, not at the level of the Ministry of Justice.

4. Therefore, until now, IT solutions were not centralized and there was no technical possibility to access the data produced by the courts.

5. The enrolment of equipment and users in a centralised system managed from outside the judiciary is a vulnerability in itself, accentuated by the possibility that computers used by court staff can be accessed from outside the judicial system. Such centralization allows, from a technical point of view, the control, manipulation or unauthorized access of the information circulating on the equipment enrolled in the domain just.ro, outside the judicial authority, without an effective supervisory mechanism on the part of this authority. The documents in progress or the information of cases could be accessed or copied, modified without the knowledge of the person responsible for the case and without the reading/modification operation being able to be identified directly, but only with the assistance of the administrator of the information system, located outside the judicial authority.

6. In this context, the Council decided to carry out an analysis on the impact of the implementation of centralized solutions, in the context of the need to respect the principle of separation of state powers and the independence of the judiciary. Until this situation is clarified, it was decided to send a letter to the courts ordering the immediate suspension of the process of enrollment in the just.ro domain of the IT equipment of the courts, as well as of the judges' accounts, and the return to the situation prior to enrollment, where this process has already been started or completed.

7. In this context, on **05.09.2024**, in the exercise of its constitutional duty to ensure respect for the independence of justice, the Section for Judges of the Superior Council of Magistracy adopted Decision no. 1519/2024 (annexed) by which it found that by enrolling computers and servers in the courts in the just.ro domain, managed by the Ministry of Justice, a vulnerability is created that is likely to affect the independence of judiciary. On this occasion, it was taken into account that the technical steps aimed at centralizing the courts' equipment and storing data centrally outside the judicial authority, cannot in any

way prevail over the guarantees of independence of the judiciary, a fundamental pillar of the rule of law.

8. In accordance with the commitment to open dialogue, on **17.09.2024**, the Superior Council of Magistracy accepted an invitation from the Ministry of Justice to participate in a meeting in order to discuss the serious constitutionality issues, highlighted by the Council, from the perspective of the intention to centralize the IT infrastructure of the courts at the level of the ministry.

During the meeting, the minister showed that a security solution that solves the vulnerabilities has already been implemented, and it is no longer possible for the Ministry of Justice to access the judges' computers. It was agreed during the respective discussions, at the level of principle, that the system envisaged to be developed cannot remain to be managed within the executive power, but must be transferred to the judicial authority, one of the options being able to involve the High Court of Cassation and Justice. At the same time, it was agreed to continue the discussions at technical level, within a working group, as well as to transmit to the ministry the written position of the Council, containing a legislative and technical analysis in which the proposed solutions would be highlighted.

9. As for the mentioned technical working group for identifying the optimal technical solution, the Council accepted the Ministry's invitation to participate in a technical meeting on **24.09.2024**.

10. On this occasion, it was found that the IT architecture proposed by the ministry involves the enrollment of ECRIS servers within the domain administered by the Ministry of Justice, and the latter will retain the privileges that allow it to continue accessing the information produced by the courts, regardless of the creation of an additional account (Enterprise) to be ceded to the High Court of Cassation and Justice.

11. As a consequence, the representatives of the Council found that the technical solution such as the one proposed by the Ministry, which involves enrolling the courts' equipment in a common domain, administered by the Ministry, even in the event of creating an Enterprise account to be taken over by the High Court of Cassation and Justice, is in direct contradiction with the principles established by the Superior Council of Magistracy by the Decision of the Section for Judges no. 1519/2024.

In these coordinates, it was considered appropriate to ask for the transfer to the Superior Council of Magistracy the attributions of the Ministry of Justice in the IT field concerning the courts, given that the digitization process requires specific technical and managerial expertise, which can be better ensured by the Council, which is composed of representatives of the courts, thus being in direct contact with the needs identified by them.

12. Thus, on **26.09.2024**, the Superior Council of Magistracy sent the Ministry of Justice Council's technical proposals in the context of the legislative framework. It was also decided to inform the High Court of Cassation and Justice about the Council's proposals, and the rest of the courts about the conclusions resulting from the activity of the technical

working group, as well as to consult them in order to establish the optimal architecture of the courts' IT infrastructure, in compliance with the principle of the independence of the judiciary.

13. In the same context, it should be emphasized that according to Law no. 303/2022, the Superior Council of Magistracy is the authority responsible for personal data.

Through the solution proposed by the ministry, it would be practically impossible for the Council to fulfill the corresponding attributions, given that it would no longer be the physical holder of the data and would no longer have direct access to them, but only intermediated access, through the administrator of the IT system, namely the Ministry of Justice.

14. Another undesirable consequence would be that the Ministry of Justice, in its capacity as administrator of the system, will become the only authority with the power to impose security policies for the system, which implicitly will lead to the possibility of establishing which IT applications can be used by the judiciary. That is in contradiction with ENCJ's Rome Declaration (2024).

15. Finally, one last remark must be made. The same process of improving the IT infrastructure was initiated by the Ministry of Justice with regard to the prosecutors' offices and, in this case, the ministry designed and accepted exactly the architecture that the Superior Council of Magistracy requests, namely a centralized architecture at the level of the Prosecutor General's Office and administered by the Prosecutor General. Basically, in the case of prosecutors, the idea that existing data should be hosted and managed within the system, and not at the level of the executive power, was accepted, while in the case of judges, this is refused without any consistent reason.

16. At present, although the situation has remained deadlocked, the Council has received informal suggestions from political level that it would be good to reach an agreement. Consistent with the openness to dialogue, the Council noted, however, that these calls envisage a possible agreement in the terms initially proposed by the Ministry, without taking into account the Council's proposals, which cannot be accepted according to the arguments previously exposed.