UNIO - *EU Law Journal*. Vol. 10, No. 2, December 2024, pp. 40-56.

School of Law - University of Minho

Digitalisation of criminal justice in the EU through eu-LISA cooperation with Eurojust and Europol: between extraordinary potential and persistent opacity

Valentina Faggiani*

ABSTRACT: The digitalisation of judicial cooperation in criminal matters and police cooperation has become one of the priorities of the EU strategy on e-Justice. The heart of this system is eu-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, and the collaborative relationship it has managed to establish with other bodies in this field, in particular Eurojust and Europol. For this very reason, after examining the role of eu-LISA, this document will focus on the main legislative instruments adopted in the Union to promote this process, which place this Agency at the centre.

KEYWORDS: digitalisation – Eurojust – eu-LISA – Europol – European Justice Strategy.

* Associate Professor of Constitutional Law at University of Granada.

1. Eu-LISA as the nerve centre for the management of large-scale IT systems in the AFSJ and synergies with Eurojust and Europol

The digitalisation of judicial cooperation in criminal matters and police cooperation has become one of the priorities of the EU strategy on e-Justice,[1] as its potential can transform the way of managing relations between legal operators in the Member States, and also with other third-party countries.[2] The heart of this system is eu-LISA,[3] the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (AFSJ), and the collaborative relationship it has established with other bodies in this field. For this reason, – after analysing the role of this Agency – this paper will focus on the main legislative instruments approved within the Union to promote the process which put it at the centre (of digitalisation).

The study of eu-LISA and its relationship with the other EU Agencies in this field, responds to the need to gain a more detailed understanding of these entities, which are an integral part of its administrative body,[4] in order to comprehend the contradictory functions and profiles, as well as the permanent tensions between the supranational perspective and intergovernmental elements, which continue to persist. These aspects limit the construction of a real "*decentralised integration*",[5] that is, the development and concrete action of cooperation systems based on the creation of "*networks*"[6] – as in the case of agencies – whose objective is to implement community policies.[7] This reasoning also allows us to reflect on whether the use and application of technology respects the fundamental rights of the people involved in a criminal process, with the confrontation between a security approach vs. the protection of personal data being very marked.

Eu-LISA is a regulatory agency, a body with legal personality and therefore "*legal, administrative and financial autonomy*",[8] based in Tallinn, Estonia, although the functions related to development and operational management are carried out in Strasbourg (France). This Agency embodies the "*delegation of operational powers*" of the

[1] Council, European e-Justice Strategy 2019-2023 (2019/C 96/04).

[2] For an overview of the digitalisation of criminal proceedings in the EU, see C. Arangüena Fanego, De Montserrat de Hoyos Sancho, Esther Pillado González (dir.) and Pedro Miguel Freitas (ed.), *El proceso penal ante una nueva realidad tecnológica europea* (Navarra: Thomson Reuters Aranzadi, 2023).

[3] Regulation (EU) 2018/1726 of 14 November 2018 on the European Union Agency for the operational management of large-scale IT systems in the area of Freedom, Security and Justice (eu-LISA), amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011, PE/29/2018/REV/1, OJ L 295, 21.11.2018, current consolidated version: 25/04/2024.

[4] On EU agencies, see E. Chiti, "European Agencies' Rulemaking: Powers, Procedures and Assessment", *European Law Journal*, vol. 19, no. 1 (2013): 93–110. J. Alberti, *Le Agenzie dell'Unione europea* (Milan: Giuffrè, 2018); M. Pi Llorens, "El nuevo mapa de las agencias europeas del Espacio de Libertad, Seguridad y Justicia", *Revista de Derecho Comunitario Europeo*, year 21, no. 56 (2017): 77-117.

[5] E. Chiti, "Diritto amministrativo europeo, stabilizzazione dei comportamenti e costruzione dell'ordine sociale", *Diritto pubblico*, no. 3 (2015): 909-984.

[6] D. Barbieri, "Agenzie Europee: un esempio di evoluzione (istituzionale) amministrativa?", *Rivista Italiana di Politiche Pubbliche*, no. 3 (2007): 77-102. See in particular page 80. The author describes the agencies also as "punti focali (nodi) di una rete di relazioni interistituzionali" that implement "modalità di coordination (formali ed informali)" (page 94).

[7] A. Akbik, C. Freudlsperger and M. Migliorati, "Differentiated participation, uniform procedures: EU agencies in direct policy implementation", *West European Politics*, vol. 47, no. 3 (2024): 645-670.

[8] Recital 5 of the eu-LISA Regulation.

EU, and more specifically of the European Commission; that is to say, the power to implement (actions/measures?) in the areas in which the Member States have decided to share powers with the Union.[9] This decentralisation process, which has led to a proliferation of agencies, has driven "*institutional transformation*", influencing the structure of the system.[10]

Even more so in the specific case where the structured exchange of data in the field of various large-scale information systems through dialogue between centre and periphery is creating a new model for managing relations in such sensitive sectors as immigration and asylum, judicial cooperation in civil and criminal matters, and police cooperation. On the other hand, and here lies the most worrying aspect, although these bodies have acquired significant powers – which are exercised in an almost autarchic manner – there are no truly incisive control mechanisms that can effectively and immediately counteract any overstepping of boundaries.

Eu-LISA, established in 2011 to strengthen cooperation between Member States in areas of the AFSJ, following the reforms of 2018 and 2024 – which extended its mandate – is currently responsible for the operational management of large-scale IT systems within the AFSJ,[11] *i.e.*, for carrying out "*all functions necessary to maintain the operation of these IT systems*", including responsibility for the communication infrastructure they use. These systems are:

- SIS II, the second-generation Schengen Information System;
- VIS, the Visa Information System;
- EURODAC, the European Fingerprint Comparison System for Asylum Seekers;
- EES, the Entry/Exit System;
- DubliNet, for the transmission of asylum applications within the EU;
- ETIAS, the European Travel Authorisation System;
- ECRIS-TCN and the ECRIS reference application, the European Criminal Records Information System – Third-Country Nationals;[12]
- e-CODEX, the computerised system for cross-border electronic data exchange in the field of judicial cooperation in civil and criminal matters;
- the collaboration platform for joint investigation teams (JITs);
- and the Prüm II router.

The aim of eu-LISA is to ensure interoperability,[13] i.e. to ensure better access to information stored in different EU information systems and to manage identity protection at the EU level. Its operational mandate can also be further extended if laid down in EU legal acts, in accordance with Articles 67 to 89 TFEU. However, it is important to emphasise that these systems "*shall not exchange data or allow the sharing*

[9] See F. Tassinari, "La institucionalización de la competencia operativa de la Unión Europea para la gestión y la interoperabilidad de los sistemas informáticos de gran magnitud del Espacio de Libertad, Seguridad y Justicia: eu-LISA", *La Ley Unión Europea*, no. 111 (2023).

[10] D. Barbieri, *op. cit*., 77.

[11] Its normative bases are found in Articles 74, 77, paragraph 2, a) and b), 78, paragraph 2, e), 79, paragraph 2, c), 82, paragraph 1, d), 85, paragraph 1, 87, paragraph 2, a), and 88, paragraph 2, of the TFEU. The extension of eu-LISA's mandate has been facilitated by the absence of a definition of large-scale systems.

[12] G. Di Paolo, "Novità: Verso una nuova architettura di gestione dei dati contenuti nei sistemi di informazione dell'Unione", *Cassazione penale*, vol. 59, no. 9 (2019): 3380-3384.

[13] F. Tassinari, "La interoperabilidad de los sistemas de información de gran magnitud de la Unión Europea y la detección de identidades múltiples: garantías y responsabilidades", in *Lucha contra la criminalidad organizada y cooperación judicial en la UE: instrumentos, límites y perspectivas en la era digital*, dir. F.J. Garrido Carrillo, ed. V. Faggiani (Junta de Andalucía: Thomson Reuters Aranzadi, 2022), 291-338.

of information or knowledge, unless specifically provided for in a Union legal act."[14] This means that eu-LISA does not "*merge*" the different systems or share information.[15] In other words, the Member States continue to manage their data at a central level, although these systems are then connected, precisely through eu-LISA, due to their decentralised nature.

In order to control the quality of data entered into the systems it manages, and without prejudice to the responsibility of the States, eu-LISA is responsible for establishing automated mechanisms and procedures, common indicators and minimum quality standards for data storage. To this end, it shall establish a central repository, containing only anonymised data for reporting and statistics.[16] Furthermore, where interoperability of large-scale information systems is envisaged, it shall develop the necessary actions[17] and monitor research for the operational management of these systems, and may carry out pilot projects.[18]

Finally, eu-LISA will provide support to Member States and the Commission by advising them on the "*connection of national systems to the central systems of the large-scale IT systems it manages.*"[19] Member States may also submit an individual request for *ad hoc* assistance to the Commission for extraordinary security or migration needs, which, if assessed positively, will be forwarded without delay to the Commission and the Management Board will be informed. In the event of a negative assessment, the Member State will be informed. The Commission may also ask the Agency to "*provide advice or support (...) on technical issues related to existing or new systems, including by way of studies and testing.*"[20]

While eu-LISA can be seen as the nerve centre for the operational management of large-scale IT systems in the Court of Justice of the European Union (CJEU), its actual functioning also depends on cooperation with the various agencies in this field, such as Eurojust, the EU agency specialised in judicial cooperation in criminal matters,[21] and Europol, the EU agency for law enforcement cooperation.[22] The synergies that have developed between these agencies have enabled important work to be carried out in accelerating the digital transformation and the uptake of AI-based IT solutions in the field of Justice and Home Affairs (JHA), laying the foundations for the application of digital systems in these areas.

---

[14] Article 1, paragraph 6, of the eu-LISA Regulation.

[15] M. Illamola Dausà, "EU-LISA, el nuevo modelo de gestión operativa de las distintas bases de datos de la UE", *Revista CIDOB d'afers internacionals*, no. 111 (2015): 109.

[16] Article 12 of the eu-LISA Regulation.

[17] Article 13 of the eu-LISA Regulation.

[18] Article 14 of the eu-LISA Regulation.

[19] Recital 8 of the eu-LISA Regulation.

[20] Article 16 of the eu-LISA Regulation.

[21] Regulation (EU) 2018/1727 of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust) and replacing and repealing Council Decision 2002/187/JHA, OJ L 295, 21.11.2018. In this regard, see: V. Faggiani, "Eurojust en la lucha contra la criminalidad organizada", in *Retos en la lucha contra la delincuencia organizada. Un estudio multidisciplinar: garantías, instrumentos y control de los beneficios económicos*, dir. F.J. Garrido Carrillo, ed. V. Faggiani (Thomson Reuters Aranzadi, 2021), 185-210.

[22] Regulation (EU) 2016/794 of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016. The last major reform was introduced by Regulation (EU) 2022/991 of 8 June 2022, PE/8/2022/REV/1, OJ L 169, 27.6.2022.

This cooperation is expressly provided for in the eu-LISA Regulation, which allows these agencies to take part as observers in the eu-LISA Management Board meetings, which are held twice a year and has been reinforced by the signing of interesting Memoranda of Understanding, the result of an ongoing dialogue.[23] Both Europol and Eurojust have entered into such agreements respectively in 2016 and 2017[24] with the aim of jointly updating existing digital systems and processes and establishing new ones, modernising the functioning of criminal justice and improving judicial cooperation in the EU.

In both cases, the Agencies have committed themselves to liaise by exchanging expertise and best practices in the implementation of their respective mandates and, where relevant, in IT-related activities and services, and in strategic and administrative matters, such as work programmes, strategies and action plans. The Memorandum between eu-LISA and Europol also makes express reference to the duty to cooperate in investigating and monitoring the development of such initiatives, *inter alia*, in the areas of IT and cybersecurity, certification, standardisation, use of biometrics, business continuity and incident analysis,[25] and to the importance of providing training to Member States and Europol and eu-LISA staff.

The exchange of personal data and data used for law enforcement purposes (including data subject to ongoing or future law enforcement activities) is excluded from the scope of the eu-LISA Memorandum with Europol, and the transmission of operational information – including data relating to an identified or identifiable person – is excluded from the scope of the eu-LISA Memorandum with Eurojust. The information exchanged is subject to a duty of confidentiality. In addition, coordination of cooperation with the other party will be carried out through the establishment of a contact point, allowing for a regular mutual exchange of information and consultation on the cooperation activities undertaken, on projects of mutual interest that may be implemented jointly, and on all other matters of common interest falling within the scope of the Memorandum of Understanding. Progress will be assessed, and new cooperation activities discussed on an annual basis.[26] Any disputes arising in relation to the interpretation or application of these Memoranda will be resolved through consultations and negotiations between representatives of the parties.[27]

---

[23] Article 22 of the eu-LISA Regulation.

[24] Memorandum of understanding between Europol and eu-LISA, 22.3.2016, https://www.eulisa.europa.eu/PartnersStakeholders/Documents/MoU_Europol_eu-LISA.pdf; Memorandum of Understanding between Eurojust and eu-LISA, 19.9.2017, https://www.eurojust.europa.eu/document/memorandum-understanding-between-eurojust-and-eu-lisa. The Memorandum between eu-LISA and Eurojust was implemented through the Cooperation Plan 2021-2023 of 11 October 2021, which has launched joint activities on sectors of mutual interest https://www.eurojust.europa.eu/document/cooperation-plan-2021-2023-eurojust-and-eu-lisa. The need to further strengthen cooperation on digitalisation has also been highlighted in: Eurojust, Press release, Eurojust and eu-LISA discuss closer cooperation to support digitalisation of justice across Europe, Joint Eurojust/eu-LISA, 7.3.2024, https://www.eurojust.europa.eu/news/eurojust-and-eu-lisa-discuss-closer-cooperation-support-digitalisation-justice-across-europe. On cooperation between eu-LISA and Eurojust, see V. Faggiani, "The European e-Justice Strategy: advancing the application of Artificial Intelligence", *Digital Law and Innovation Review*, no. 19 (2024).

[25] Article 4 of the Memorandum of understanding eu-LISA-Europol.

[26] Article 10 of the Memorandum of understanding eu-LISA-Eurojust and Article 9 of the Memorandum of understanding eu-LISA-Europol.

[27] Article 11 of the Memorandum of understanding eu-LISA-Eurojust and Article 10 of the Memorandum of understanding eu-LISA-Europol. Eu-Lisa and Eurojust, Joint Report: Artificial intelligence supporting cross-border cooperation in criminal justice, 22.7.2022, https://www.eurojust.

It is very interesting to highlight that this fruitful collaboration, which has been developed previously at the operational level, from the implementation of soft law acts, good practices and protocols, has materialised in the adoption of interesting legislative measures, which constitute an integral part of the digitalisation package of justice[28] and in the Regulation on AI of biometric recognition systems in law enforcement activities.[29]

2. The platform on joint investigation teams as a strategic instrument in the fight against organised crime

As regards cooperation between eu-LISA and Eurojust, it is worth highlighting the Regulation establishing a collaboration platform for JITs and the redesigned Eurojust Case Management System, equipped with AI-based components. JITs[30] allow judicial, police and customs authorities from two or more Member States, and in some cases from third countries, to cooperate and communicate directly. These mechanisms, which respond to a common investigation strategy, are one of the most advanced instruments of judicial cooperation in criminal matters, being a working forum for judges and prosecutors and police authorities. They are established by virtue of an agreement between the competent authorities of two (bilateral action) or more States (multilateral action) for the purpose of carrying out criminal investigations. They usually work for a period ranging from 12 to 24 months, depending on the complexity of the matter in question and therefore the time required for the investigation.

The establishment of a platform, such as that provided for by Regulation (EU) 2023/969,[31] can greatly facilitate collaboration between members of the JITs so that they can organise the "*investigation and prosecution*"[32] of cross-border crimes, such as cybercrime, terrorism and serious and organised crime, by reducing lengthy procedures and formalities. The need to put in place such a measure is explained in the light of Regulation (EU) 2022/838,[33] which has given Eurojust the task of preserving, analysing and retaining in an automated temporary data management and storage

europa.eu/publication/artificial-intelligence-supporting-cross-border-cooperation-criminal-justice.

[28] European Commission, Communication: "The digitalisation of justice in the EU: A range of opportunities", 2.12.2020, COM/2020/710 final.

[29] Article 5 of Regulation (EU) 2024/1689 of 13 June 2024 establishing harmonised rules on artificial intelligence (Artificial Intelligence Regulation), PE/24/2024/REV/1, OJ L, 2024/1689, 12.7.2024.

[30] See Council Framework Decision of 13 June 2002 on joint investigation teams, OJ L 162, 20.6.2002. Pursuant to Article 1 of this Framework Decision: "The competent authorities of two or more Member States may, by common agreement, establish a joint investigation team, for a specified purpose and for a limited period which may be extended with the consent of all parties, for the purpose of carrying out criminal investigations in one or more of the Member States which established the team."

[31] Regulation (EU) 2023/969 of 10 May 2023 establishing a collaboration platform to support the functioning of joint investigation teams and amending Regulation (EU) 2018/1726, PE/73/2022/REV/1, OJ L 132, 17.5.2023. This Regulation has been adopted pursuant to Article 82(1)(d) TFEU.

[32] Recital 3 of Regulation (EU) 2023/969.

[33] Regulation (EU) 2022/838 of 30 May 2022 amending Regulation (EU) 2018/1727 as regards the preservation, analysis and storage at Eurojust of evidence relating to genocide, crimes against humanity, war crimes and related criminal offences, OJ, No. 148, 31.5.2022. Specifically, Article 4, para. 1 of Regulation (EU) 2018/1727 was amended. Aside from its importance in the context of the conflict in Ukraine, this reform has given Eurojust greater relevance in the fight against cases of serious cross-border crime. See M. Torres Pérez, "Eurojust, veinte años de compromiso por la cooperación judicial penal en Europa. el futuro de la Agencia ante la guerra en Ucrania", *Revista Electrónica de Estudios Internacionales*, no. 44 (2022): 199-201. 1-17.

facility evidence relating to genocide, crimes against humanity, war crimes and related criminal offences, until a new system is operational. This has enabled the exchange of relevant evidence with the competent national authorities and international judicial authorities, in particular the International Criminal Court, in order to ensure that the perpetrators of crimes committed in Ukraine do not go unpunished but are held accountable.[34] Following this amendment, a Centre for the Prosecution of the Crime of Aggression against Ukraine managed by Eurojust was established in July 2023 and operates through investigative teams, which can collaborate on a voluntary basis. By July 2023, Lithuania, Latvia, Estonia, Poland and Romania had joined, and the International Criminal Court (ICC) itself is also involved.

The purpose of the JIT collaboration platform is to facilitate the exchange of information and to conduct communication, indicating the *modus procedendi*. It is an enabling system to allow the EU to develop a *"coordinated response"* to criminal activities and to support Member States in the fight against crime. The JIT collaboration IT platform, which will be voluntary, will be hosted by eu-LISA, which will be responsible for the design of the physical architecture, for development in accordance with the principle of data protection by design and by default, for operational management to ensure its maintenance, and for its proper running,[35] using the existing functions of SIENA (Secure Information Exchange Network) and other Europol attributions to ensure complementarity and, where appropriate, connectivity.[36]

The platform will consist of:

a) a centralised information system, allowing temporary storage of data for the time necessary to transfer it. Such information must be automatically and permanently deleted once downloaded by all recipients;

b) communication software allowing secure local storage of data on users' devices;

c) a connection between the centralised information system and the relevant IT tools supporting the operation of the ECIs and managed by the ECI Network Secretariat.

The purpose of this tool is:[37]

a. to facilitate the coordination and management of the ECIs;

b. to facilitate the rapid and secure exchange and temporary storage of operational data, including large files, through an upload and download function, and of non-operational data between users;

c. to ensure secure communications through a functionality including instant messaging, chat, audio and video conferencing;

d. enable traceability of evidence exchanges, using an advanced recording and tracking mechanism, as well as access to and processing of evidence;

e. the evaluation of ECIs, through a specific collaborative process.

The European Commission will have to take a decision to activate the platform by 7 December 2025. Within this framework, eu-LISA will make the communication software available to users of the JIT collaboration platform. It will also provide training on its technical use to the JIT network secretariat, provide training material and set up a helpdesk to respond to the consequences of any technical incidents.

[34] Since 2016, Eurojust has had a cooperation agreement with Ukraine under which a Ukrainian liaison prosecutor is based in Europe to facilitate cooperation.

[35] Article 7 of Regulation (EU) 2023/969.

[36] Recital 22 of Regulation (EU) 2023/969.

[37] Article 5 of Regulation (EU) 2023/969.

As regards its internal management, the Governing Board, which is the executive body of eu-LISA, shall constitute the Programme's Governing Board, which shall be responsible for managing the design and development phase of the platform.[38] The Programme's Governing Board shall submit regular, and where possible monthly, written progress reports to the eu-LISA Governing Board. It shall have no decision-making powers and no mandate to represent the members of the eu-LISA Governing Board. Furthermore, eu-LISA shall set up the Advisory Group to acquire expertise and to prepare the annual work programme and annual activity report of the agency.[39] The Advisory Group shall be composed of representatives of the Member States, the Commission and the Secretariat of the ECI network. It shall be chaired by eu-LISA.

The ECIs are conceived as a space that users can enter upon prior authorisation from the administrator(s), who manage access to the operational and post-operational phases, in accordance with the agreement to be stipulated.[40] It will be essential to ensure the security of data exchange through the use of "*strong end-to-end encryption algorithms to encrypt data in transit or at rest.*"[41] The operational data of the ECIs will be kept in the centralised information system for the time necessary for their download by the users of said platform. After this process or once the retention period has expired, the data will be automatically and permanently deleted from the centralised information system.[42] Non-operational data will be stored until the conclusion of the evaluation of the ECI, and in any case for no more than five years from its entry into the platform. If the evaluation is not planned or after the expiration of the retention period, they will be automatically deleted from the centralised computer system.[43]

The controllers of personal data are the competent national authority of a Member State and, where applicable, Eurojust, Europol, the European Public Prosecutor's Office, OLAF or any other Union body, office or agency. In addition, a JIT Space Administrator shall be designated as controller where third countries or representatives of international judicial authorities are involved in the JIT Collaboration Platform.[44] Eu-LISA shall be responsible for the processing of personal data exchanged through and stored on the JIT Collaboration Platform. To this end, it shall ensure that access to the system and all data processing operations are logged in order to monitor the integrity and security of the data and the lawfulness of such processing and to carry out internal oversight. The Agency shall not have access to operational and non-operational data stored in the JIT Collaboration Spaces[45] and shall respect professional secrecy and confidentiality obligations. Users of the Platform shall be considered joint controllers of non-operational personal data. Compliance with eu-LISA obligations is monitored and assessed on the basis of the various reports to be submitted[46], which are the main instrument in this regard.

[38] Recital 28 of Regulation (EU) 2023/969.
[39] Article 12 of Regulation (EU) 2023/969.
[40] Recital 29 of Regulation (EU) 2023/969.
[41] Recital 30 of Regulation (EU) 2023/969.
[42] Article 21 of Regulation (EU) 2023/969.
[43] Article 22 of Regulation (EU) 2023/969.
[44] Article 23 of Regulation (EU) 2023/969.
[45] Recital 37 of Regulation (EU) 2023/969.
[46] Regarding the reports to be submitted by eu-LISA and the Commission for monitoring the development and operation of the ECI platform, reference is made to Recitals 23 and 38 and to Article 26 of Regulation (EU) 2023/969.

Finally, a Member State, Eurojust, Europol,[47] the European Public Prosecutor's Office, OLAF or any other competent Union body or agency shall be liable for damage caused to the JIT collaboration platform by failure to fulfil its obligations, unless eu-LISA has not taken reasonable measures to prevent such damage from occurring or to minimise its consequences. In the event that the State is liable, the national law of that Member State shall apply, and in all other cases the constituent acts of the other bodies shall apply.[48]

3. The terrorism case management system

The new terrorism case management system, established by Regulation (EU) 2023/2131 of 4 October 2023 amending the Eurojust Regulation,[49] is also based on a decentralised IT system for the secure exchange of data, which will be connected to a network of interoperable computer systems (back-end) and e-CODEX access points.[50]

The aim is to facilitate the transmission of information between the authorities of the Member States and, where appropriate, with third countries to Eurojust in order to enable the Agency to identify certain links between cross-border judicial proceedings against suspects of terrorist offences, as well as with information processed at Eurojust relating to other cases of serious crime, which require the adoption of cooperation measures.[51]

Indeed, a person suspected or accused in a case pending in one Member State may have been involved in a case already concluded in another Member State, whether with a conviction, acquittal or dismissal, and there may also be links between investigations or enquiries that would not otherwise have been apparent, making it necessary to retain data relating to all types of investigation, not only those that have ended with a conviction.

It is therefore very important to take into account the dynamic and global nature of transnational crime, which may affect two or more States and may be discovered at a later stage, requiring the establishment of forms of coordination

[47] In relation to Europol, see, for example, Judgment CJEU (GC) *M. Kočner v. Europol*, 5 March 2024, C-755/21 P, ECLI:EU:C:2024:202, annulling Judgment CJEU *Kočner v. Europol*, of 29 September 2021, T-528/20, ECLI:EU:T:2021:631, and ordering Europol to compensate the appellant for the damage suffered as a result of the disclosure of personal data and the inclusion of her name on the "mafia lists."

[48] Article 20 of Regulation (EU) 2023/969.

[49] See in particular Art. 22a of Regulation (EU) 2023/2131 of 4 October 2023 amending Regulation (EU) 2018/1727 and Council Decision 2005/671/JHA as regards the exchange of digital information in terrorism cases, OJ L, 11.10.2023. Eurojust, EJ20 Anniversary essays, AI and data protection in judicial cooperation in criminal matters, https://www.eurojust.europa.eu/20-years-of-eurojust/ai-and-data-protection-judicial-cooperation-criminal-matters.

[50] Regulation (EU) 2022/850 of 30 May 2022 on a computerised system for cross-border electronic exchange of data in the field of judicial cooperation in civil and criminal matters (e-CODEX system) and amending Regulation (EU) 2018/1726, OJ L 150, 1.6.2022. In line with the principle of interoperability, the e-CODEX system enables the justice sector to connect to the IT systems of competent national authorities, such as the judiciary, or other organisations. Pursuant to Art. 3.1 of Regulation (EU) 2022/850, the e-CODEX system (system for communication for digital justice by electronic data interchange) means a decentralised and interoperable system for cross-border communication to facilitate the electronic exchange of data, in particular any content transferable in electronic form, in a rapid, secure and reliable manner in the field of judicial cooperation in civil and criminal matters.

[51] Recital 9 of Regulation (EU) 2023/2131.

and collaboration between the competent authorities.[52] To do so, they "*need to know exactly what kind of information they have to transmit, at what stage of the national criminal proceedings and in which cases*."[53] In addition, this information must be exchanged in a structured, organised, systematic and semi-automated manner, that is to say partly automated and partly controlled by people.[54]

This is a "*modernised*" case management system, which is intended to integrate, improve and facilitate the European Counter-Terrorism Register (CTR)[55] by making up for its shortcomings. Indeed, having been established after the adoption of the Eurojust Regulation – Regulation (EU) 2018/1727 –, this regulation did not mention it nor is it integrated into its structure, which did not allow for cross-data exchange. It was therefore necessary to improve Eurojust's ability to detect links and compare biometric data, since the transmission of structured data reduces administrative burdens and the quality of the results of information matching.[56]

This digital infrastructure will integrate the CTR, transmitting information to it, so that it can store data and exchange information across borders regarding pending criminal investigations and proceedings against persons suspected of terrorism.[57] The detection of such links between terrorism investigations and criminal proceedings and the retention of this data by Eurojust is essential.

In these cases, biometric data represents the only link with these persons, given that third-country nationals often use false or double identities,[58] and its transmission is decisive, although with due caution to avoid violating the right to private and family life and to personal data (Articles 7 and 8 of the Charter), and only for the purpose of identifying persons involved in criminal proceedings for terrorist offences.

The competent national authorities are obliged to share information with Eurojust as soon as possible and to endeavour to update the system, except at the earliest procedural stage, where it may jeopardise ongoing investigations or the safety of a person, or where it would be contrary to essential security interests of the Member State concerned.[59]

The following objectives are intended to be achieved:[60]

"(a) support the management and coordination of investigations and prosecutions for which Eurojust is providing assistance;

(b) ensure secure access to and exchange of information on ongoing investigations and prosecutions;

(c) allow for the cross-checking of information and identifying links;

(d) allow for the extraction of data for operational and statistical purposes;

---

[52] Article 85 TFEU and recital 25 of Regulation (EU) 2023/2131.

[53] Recital 10 of Regulation (EU) 2023/2131.

[54] Recital 10 of Regulation (EU) 2023/2131.

[55] In September 2019, on the basis of Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation in respect of terrorist offences, OJ L 253, 29.9.2005, Eurojust set up the European Judicial Counter-Terrorism Register in order to identify links between judicial proceedings against suspects of terrorist offences and the resulting coordination needs. Eurojust, Press Release. Setting up of judicial counter-terrorism register at Eurojust, 20.6.2019. Available at https://www.eurojust.europa.eu/news/setting-judicial-counter-terrorism-register-eurojust.

[56] Recital 22 of Regulation (EU) 2023/2131.

[57] Article 23 of Regulation (EU) 2023/2131.

[58] Recital 13 of Regulation (EU) 2023/2131.

[59] Recital 17 of Regulation (EU) 2023/2131.

[60] Article 23 of Regulation (EU) 2023/2131.

(e) facilitate monitoring to ensure that the processing of operational personal data is lawful and complies with this Regulation and the applicable data protection rules."

Secure digital communication and data exchange between national and competent authorities and Eurojust will be carried out through the decentralised IT system.[61] The case management system will be connected to a network of interoperable e-CODEX IT systems and access points, operating under the individual responsibility and management of each Member State and Eurojust to enable a secure and reliable cross-border exchange of information. Where this is not possible due to the unavailability of the decentralised IT system or exceptional circumstances, it will be carried out by the fastest and most appropriate alternative means, ensuring its reliability and offering an equivalent level of security and data protection.

The competent national authorities shall transmit information to Eurojust in a semi-automated and structured manner,[62] as provided for in the implementing act to be adopted by the Commission. The Commission shall also be responsible for the creation, maintenance and development of a reference application software which Member States and Eurojust may decide to use as a back-end system, which is packaged and delivered separately from the e-CODEX components necessary to connect it to the decentralised IT system. Such a set-up will allow Member States to re-use or enhance their existing national judicial communication infrastructures for cross-border use and enable Eurojust to connect its case management system to the decentralised IT system.

4. Digitalisation of cross-border judicial cooperation in civil, commercial and criminal matters through e-CODEX

In this regard, the Regulation[63] and the Directive[64] on the digitalisation of cross-border judicial cooperation in civil, commercial and criminal matters in the EU aim to create a *"harmonised model"*,[65] based on a *"uniform legal framework for the use of electronic communication between competent authorities"* in such proceedings.[66] In this way, the EU attempts to give specificity to the principles of data protection by design and *"digital by default"*,[67] which includes information that can be read automatically,

[61] Article 22a of Regulation (EU) 2023/2131.

[62] Articles 21 and 21a of Regulation (EU) 2023/2131.

[63] Regulation (EU) 2023/2844 of 13 December 2023 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters and amending certain legal acts in the field of judicial cooperation, OJ, 2844, 27, 12.2023. The new regulations affect numerous legal acts. With regard to acts in the field of judicial cooperation in criminal matters, see Annex II.

[64] Directive 2023/2843 of 13 December 2023 amending Directives 2011/99/EU and 2014/41/EU, Directive 2003/8/EC and Framework Decisions 2002/584/JHA, 2003/577/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA, 2008/947/JHA, 2009/829/JHA and 2009/948/JHA as regards the digitalisation of judicial cooperation, OJ L, 2023/2843, 27.12.2023. Similarly to the Regulation, the Directive on the digitalisation of judicial cooperation has also modified a series of acts in criminal matters to adapt them to the digital context and to specify the changes introduced by the Regulation to standardise the regulations in this area and provide it with greater legal certainty.

[65] Recital 58 of Regulation (EU) 2023/2844 uses the expression "harmonised digitalisation of cross-border judicial cooperation." On these measures, see F. Gascón Inchausti, "The new regulation on the digitalisation of judicial cooperation in the European Union: something old, something new, something borrowed and something blue", *ERA Forum*, 24 (2024): 535-552.

[66] Article 1 of Regulation (EU) 2023/2844.

[67] Recital 1 of Regulation (EU) 2023/2844. In the Digital Market Strategy for Europe, EU eGovernment Action Plan 2016 – 2020 – Accelerating the digital transformation of government, Brussels, 19.4.2016,

in order to offer preferential services in digital form, while keeping other channels open for those who cannot or do not want to connect.

The modernisation of EU cross-border procedures rules provides the system with increased efficiency and effectiveness, facilitating access to justice, reducing the administrative burden and processing times and giving authorities greater ability to react to cases of force majeure. These positive aspects reinforce the EU strategy in the fight against cross-border criminal cases, ensuring a high level of security.

However, efficiency in electronic data exchange cannot be at the expense of the guarantees necessary to avoid social exclusion, but must ensure mutual trust, interoperability, security and the fundamental rights and freedoms of all persons concerned.[68] To this end, *"a network of IT systems and interoperable access points"* will be established, under the individual responsibility and management of each Member State, body, office or agency of the Union.[69] Its access points will be based on e-CODEX,[70] which becomes the imputation centre of this decentralised system, with eu-LISA also assuming responsibility for this system.

The use of a decentralised computer system is mandatory unless it is impossible due to a system interruption, or due to the characteristics of the information, such as in the case of material evidence or the need to analyse an original paper document to verify its authenticity or due to situations of *force majeure.*[71] In these cases, the most appropriate alternative means of communication must be chosen in terms of speed and security, such as by postal service or in-person transmission. Likewise, there may be situations in which the authorities need direct, less formal personal communication,[72] such as through email, or other means of communication due to the need to process particularly sensitive data.[73]

For oral hearings, the optional use of videoconferencing or other remote communication technologies is provided for in order to verify the identity of the person who has to make a statement and to facilitate audiovisual, audio and oral communication during the hearing.[74] The procedure in this regard shall comply with the law of the Member State in which this procedure is carried out and which has requested the use of remote communication technologies.[75] In *"exceptional circumstances"*, where there is a serious threat to public health or security that is real and present or foreseeable,[76] exceptions may be made to the need to obtain the consent of the person concerned by the use of the technologies. Where consent is not requested, suspects, accused or convicted persons or the person concerned may request a re-examination in accordance with the provisions of national law. This is without prejudice to possible violations of the fundamental rights of those affected and the right to effective judicial protection.[77]

COM(2016) 179 final, the 7 key principles have been indicated: digital by default, once-only principle, inclusion and accessibility, openness and transparency, cross-border by default, interoperability by default, trust and security.

[68] Recitals 5, 6 and 7 of Regulation (EU) 2023/2844.

[69] Article 2(3) of Regulation (EU) 2023/2844.

[70] Recital 20 of Regulation (EU) 2023/2844.

[71] Recital 24 of Regulation (EU) 2023/2844.

[72] Recital 25 of Regulation (EU) 2023/2844.

[73] Article 3 of Regulation (EU) 2023/2844.

[74] Recitals 31 and 32 and art. 6 of Regulation (EU) 2023/2844.

[75] Recital 42 of Regulation (EU) 2023/2844.

[76] Recital 44 of Regulation (EU) 2023/2844.

[77] Article 47 of the Charter and recital 45 of Regulation (EU) 2023/2844.

5. The Prüm II system as a response to the free movement of criminals through the free movement of data

The Prüm II Regulation, adopted in March 2024 [Regulation (EU) 2024/982], on automated searches and exchange of data for the purposes of police cooperation,[78] amends the previous system. In this way, the security approach is reinforced and with it the role of both the Member States and Europol, whose liaison point is represented by eu-LISA. This is a very interesting, but also disturbing, example of how data exchange through digitalisation is transforming the way law enforcement activities and cooperation[79] are carried out and communicated to identify persons involved in the commission of a crime with transnational elements.

This measure is certainly timely. It is enough to think that this extraterritorial scope of crime creates links between different places and the perpetrator of the crime, developing a space of free movement of criminals to which the free movement of data on these persons must be responded to between the authorities competent in the investigation, detection and prosecution of crime, which should also operate in a space without borders. According to the data, *"in 2021, it was found that more than 70% of criminal organisations were present in more than three Member States."*[80] The Prüm II Regulation, together with the Directive on the exchange of information between judicial authorities of the Member States,[81] aims to make up for the deficiencies of the current system in relation to the lack of direct communication in the exchange of data, the existence of loopholes, the lack of harmonisation and compliance with the regulations by certain Member States, which end up benefiting criminals.[82]

The Prüm II system is based on police cooperation. Its bases are Article 87(2) TFEU, its purpose being to facilitate the exchange of personal data between the competent authorities, and Article 88(2) TFEU on the role of Europol in relation to the reinforcement of internal security. These precepts, in turn, have to be balanced with the right to the protection of personal data, provided for in Articles 16 TFEU, 8 of the European Convention on Human Rights (ECHR) and Article 7 of the Charter, which, according to the jurisprudence of the CJEU,[83] is not conceived as an absolute right, but must be considered taking into account its function in society and Directive 2016/680.[84] The regulation by the EU of these aspects does not affect the exclusive competence of the States over their own national DNA databases.[85] As

[78] Regulation (EU) 2024/982 of 13 March 2024 on automated searching and exchange of data for the purposes of law enforcement cooperation and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) 2019/817 and (EU) 2019/818 (Prüm II Regulation), PE/75/2023/REV/1, OJ L 2024/982, 5.4.2024.
[79] EU Strategy for a Security Union 2020, COM(2020) 605 final, 24.7.2020.
[80] EU Serious and Organised Crime Threat Assessment 2021, SOCTA, 12 April 2021.
[81] Directive 2023/977 of 10 May 2023 on the exchange of information between Member States' customs and law enforcement authorities and repealing Council Framework Decision 2006/960/JHA, OJEU, No 134, of 22 May 2023.
[82] EU Strategy against Organised Crime 2021-2025, COM(2021) 170 final of 14.4.2021.
[83] Among others, see Judgment CJEU *FT and DW*, 26 October 2023, C-307/22, ECLI:EU:C:2023:811.
[84] Directive 2016/680 of 27 April 2016 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, OJ L 119, 4.5.2016.
[85] Recital 12 of Regulation (EU) 2024/982.

regards the normative source, the regulation was chosen due to the need for this regulation to be directly and uniformly applicable in all Member States.

In this way, on the one hand, Member States will be able to automatically check biometric data from third countries held by Europol and make them available to law enforcement authorities. On the other hand, Europol, which will be an integral part of the Prüm framework, will be able to compare data from third countries on criminals and terrorists with those held in the national databases of the Member States, establishing links.[86]

More specifically, the regulation regulates "*the automated searching of DNA profiles, dactyloscopic data, certain vehicle registration data, facial images and police records*",[87] to allow the exchange of information between law enforcement authorities on persons involved in criminal proceedings as suspects and accused persons and/or missing persons in the context of criminal investigations or for humanitarian reasons and the identification of human remains.

For this purpose, the Prüm II router and EPRIS (European Police Records Index System)[88] will be created, which act as connection points between the Member States so that they can communicate with each other by accessing this intermediation system. EPRIS responds to the principle of privacy protection by design, of which pseudonymisation represents one of the main guarantees, since the indexes and queries do not contain readable personal data, but alphanumeric strings. The system will not affect ECRIS. In addition, data on persons from third countries and held by Europol are also incorporated to make them available to the Member States.[89]

The system is a hybrid approach, between decentralised and centralised, with no central data storage. This means that there will not be a single European platform, but that the Member States will continue to control their own national platforms, which will be connected to each other via a router, from which they can request information on a particular subject and which this router will try to collect from the other Member States. Participation in these procedures and the automated exchange of police records are voluntary and respect the principle of reciprocity.

In addition, for the automated search of vehicle registration data, the Member States and Europol must use the European vehicle and driving licence information system EUCARIS, which is intergovernmental in nature, connecting all participating Member States via a network. In this case, communication is not carried out via a centralising element, but each Member State can communicate with the other connected Member States and with Europol.[90] In all this, eu-LISA will receive information from Member States on fingerprint data search capabilities[91] and on any unavailability of automated data exchange, in order to put in place alternative measures, and will keep a record of all data processing operations carried out through the router.[92]

---

[86] On the role of Europol following the 2022 reform, see V. Faggiani, "The European Strategy on e-Justice: progress in the application of Artificial Intelligence", cit.; F. Tassinari, "Issues of consistency and complementarity in EU privacy law: the europol's big data challenge", General Journal of European Law, no. 63 (2024).

[87] Recital 8 of Regulation (EU) 2024/982.

[88] Article 42 of Regulation (EU) 2024/982.

[89] Recitals 18 and 19 of Regulation (EU) 2024/982.

[90] Recital 15 of Regulation (EU) 2024/982.

[91] Article 14 of Regulation (EU) 2024/982.

[92] Articles 40 and 41 of Regulation (EU) 2024/982.

The data received will be processed by a Member State or by Europol for the purposes of the Regulation without obtaining prior consent from the State which provided the data.[93] Following the automated response to the query, the data received by a Member State or by Europol will be deleted immediately, unless further processing is required or without prior consent. Such data will be flagged if the data subject contests the accuracy of the data, which is held by a Member State or by Europol or if the latter cannot ensure its accuracy. Member States or Europol may delete such data subject to prior consent or pursuant to a decision by the competent court, supervisory authority or European Data Protection Supervisor (EDPS).

The processing of data and the adoption of the necessary measures in relation to the router will be the responsibility of eu-LISA and Europol will deal with personal data through EPRIS.[94] The competent authorities of the Member States, eu-LISA and Europol have to ensure the security of the processing by cooperating and taking the necessary measures to physically protect the data, preventing access, consultation or introduction of data by unauthorised persons.[95] In the event of a security incident affecting the router, they will cooperate with each other to ensure a response. Eu-LISA will notify any problem that arises to the Cybersecurity Service of the Union institutions, bodies, offices and agencies (CERT-EU). States will provide for effective, proportionate and dissuasive sanctions to respond to any misuse of data, processing or sharing. Liability arising from failure to comply with the obligations will be incumbent on the State concerned or Europol, unless they have taken appropriate measures to prevent this from happening or to mitigate its effects.[96]

The EDPS shall at least every four years carry out an audit of the operations relating to the processing of personal data processed by eu-LISA and Europol, the results of which shall be set out in a report to the European Parliament, the Council, the Commission, the Member States and the Union agency concerned.[97] Eu-LISA and Europol may make comments before the reports are adopted.

Finally, as regards responsibilities, the central structure during the design and development phase of the router and the technical adaptations will be hosted by eu-LISA.[98] The design will be approved by the eu-LISA Management Board, following a favourable opinion from the Commission. The Programme Management Board will submit monthly written progress reports to the eu-LISA Management Board. However, it will not have any decision-making powers, nor any mandate to represent the members of the eu-LISA Management Board. The Interoperability Advisory Group will meet regularly until the router is operational. It will report to the Programme Management Board after each of its meetings, provide the necessary technical expertise to support it in its tasks and monitor the state of readiness of Member States. And after the router's entry into operation (Article 67), eu-LISA will be responsible for the technical management of the router's core infrastructure, including its maintenance and technological developments.[99]

[93] Article 50 of Regulation (EU) 2024/982.
[94] Article 52 of Regulation (EU) 2024/982.
[95] Article 53 of Regulation (EU) 2024/982.
[96] Articles 54-57 of Regulation (EU) 2024/982.
[97] Article 58 of Regulation (EU) 2024/982.
[98] Article 66 of Regulation (EU) 2024/982.
[99] Article 67 of Regulation (EU) 2024/982.

Conclusion

In the last year, the EU has adopted some very interesting measures that will allow it to consolidate a digitalised model of judicial and police cooperation, in accordance with the European Strategy on e-Justice. The nerve centre of this system is represented by eu-LISA, the EU Agency, which is responsible for hosting and managing large-scale computer systems, and by the relationship that it has managed to develop with the other agencies of the European Justice Area, in particular Eurojust and Europol. This fruitful collaboration, which was previously carried out at the operational level, from the implementation of soft law acts, good practices and protocols, has grown in recent years, promoting the adoption of legislative acts, which have been analysed in this contribution.

In this way, mechanisms have been established that will strengthen the fight against organised crime, making the system more effective, and facilitating communication and the transmission of information between the authorities of the Member States and also third States. This contribution has analysed the collaboration platform for the ECI, the terrorism case management system, the digitalisation of communication tools in cross-border judicial cooperation in civil, commercial and criminal matters and the Prüm II system, which aims to respond to the free movement of criminals through free movement and the automated exchange of data.[100]

However, this high level of technologisation has as a counterpart the risks arising from the use of biometric data, and possible errors and discrimination due to bias.[101] In this sense, we have to read the impact of the use of data of this type in relation to the recent entry into force of the EU Regulation establishing harmonised rules on AI, which provides for the use of remote *"real-time"* biometric identification systems in public spaces for the purposes of ensuring compliance with the law, insofar as such use is strictly necessary for the purposes of investigation and prosecution of crimes, indicated in Article 5, paragraph 1, h, to verify the identity of the person. The counterpart of the use of such intrusive technology is the development of a society of control and surveillance.

On the other hand, in addition to the problems arising from the autarkic nature of technology, which makes it uncontrollable and highly invasive of fundamental rights, one cannot ignore the concerns also raised by the process of *"agencification"*, *i.e.*, the delegation of powers to EU agencies to carry out EU policies. The extraordinary potential of eu-LISA's management of large-scale IT systems, which are fuelled by AI-based mechanisms, and the important role also assumed by the other AFSJ agencies, which will undoubtedly facilitate law enforcement activities, are tempered by opacity. In this sense, these activities are often characterised by a lack of transparency, with no truly effective control and accountability instruments in place. It is enough to think that the reports issued by these bodies and by the European Commission continue to constitute purely political control mechanisms.[102]

[100] For a critique of Prüm II, see EDRI, "Automated data exchange in Prüm II: The EU's securitisation mindset keeps encroaching on our fundamental rights", 6.2.2024.
[101] EDPS, Opinion on the Commission's Proposal for the Regulation on automated data exchange for police cooperation ("Prüm II"), www.edps.europa.eu/system/files/2022-03/22-03-07_opinion-4-2022_prum_en.pdf, 2.3.2022.
[102] M. Pacini, "I regimi e la prassi di accountability di Europol ed Eurojust", Rivista italiana di diritto *pubblico comunitario*, vol. 28, no. 6 (2018): 1053-1072.

In short, the fact that 80% of crimes involve digital elements may be quite indicative of the proportions of the technological dimension of crime[103] and the need to respond to the digitalisation of criminality with the digitalisation of justice. These figures are also destined to continue increasing. However, this desire for modernisation and the commitment to the application of AI for the sake of supposed effectiveness and efficiency[104] of judicial systems cannot be at the expense of the structural principles of our legal systems. Although we live in a fluid context, characterised by continuous changes, there are insurmountable principles (Article 2 TEU), which must be preserved because otherwise the model of the Constitutional State of Law in its basic core would end up being undermined.[105]

[103] European Commission, Press Release: Fighting organised crime: New five-year strategy to boost EU-wide cooperation and improve the use of digital tools in investigations, Brussels, 14 April 2021. For the latest trends in this area, see also Internet Organised Crime Threat Assessment (IOCTA) 2024, https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024, 22.7.2024.

[104] S. Barona Vilar speaks about the process of liquefaction of the criminal justice model, "Mutación de la justicia en el siglo XXI. Elementos para una mirada poliédrica de la tutela de la ciudadanía", *Justicia poliédrica en periodo de mudanza: Nuevos conceptos, nuevos sujetos, nuevos instrumentos y nueva intensidad*, ed. S. Barona Vilar (Valencia: Tirant lo Blanch, 2022), 31-62, or also of a "liquid" or "liquidable" criminal process, faster but also less guarantor-like, ID, "Justicia penal líquida (desde la mirada de Bauman)", *Teoría y derecho: revista de pensamiento jurídico*, no. 22 (2017): 64-91.

[105] M. Brenner et al., "Constitutional Dimensions of Predictive Algorithms in Criminal Justice," *Harvard Civil Rights-Civil Liberties Law Review*, vol. 55, no. 1 (2020): 267-310; V. Faggiani, "El derecho a un proceso con todas las garantías ante los cambios de paradigma de la inteligencia artificial", *Teoría y realidad constitucional*, no. 50 (Issue dedicated to the Judicial Branch) (2022): 517-546.