AI and data protection in judicial cooperation in criminal matters

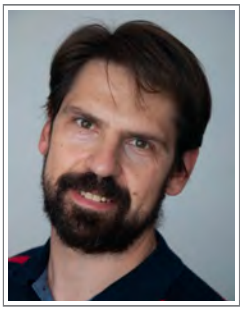
Wojciech Wiewiórowski

European Data Protection Supervisor

Michał Fila

Legal Officer at the European Data Protection Supervisor

© Wojciech Wiewiórowski



© Michał Fila

Introduction

As we celebrate the 20th Anniversary of Eurojust, the European body for judicial cooperation in criminal matters, we should also review the historical and technological contexts in which the agency began its existence.

The year is 2002: the European Union consists of 14 Member States; new Euro banknotes and coins are in our pockets; the future of the Nice Treaty in the period between Irish referendums is uncertain; the role of the year-old Charter of Fundamental Rights is uncertain as well; and expectations are high for the newly established European Convention led by Valéry Giscard d'Estaing, who was in charge of writing the Constitution for Europe. We were also just four months on from 9/11. Internet Explorer was occupying more than 90% of the market; Safari and Firefox did not yet exist. Using your European mobile phone (smartphones were not yet known) in the United States or Japan was difficult and barely affordable. The IT market was recovering after the dot.com bubble collapse.

What were we, the authors, doing 20 years ago? In 2002, Wojciech was teaching constitutional and European law as a young PhD student, exploring the interplay between IT and law, both academically and professionally. Michał was defending his Master of Laws (LL.M) thesis on police cooperation in Europe at the Christian Albrecht University in Kiel, Germany. Our interest in the newly created Eurojust was limited. Although some specific and focused solutions, developed by artificial intelligence (AI) researchers, were being widely used at that time, they were still only rarely described as 'artificial intelligence'. The only remote association made between the judiciary and AI in popular culture was probably through the figure of Judge Dredd!

Fast forward to 2022 and here we are, with national strategies, policies and regulations on AI adopted by almost all major economies in the world. Non-binding guidelines or principles for the use of AI, focusing on ethical considerations, are common. Proposals for legal changes to address issues raised by AI (for example, transparency) are tabled in the European Union, the United Kingdom, the United States and around the globe. At the same time, Wojciech is at the helm of the EU's supervisory authority responsible for monitoring compliance with data protection rules by all EU institutions, offices, bodies and agencies (EUIs), including, since December 2019, Eurojust. Since September 2020, Michał has been the legal officer at the European Data Protection Supervisor (EDPS) responsible for relations with Eurojust.

The EDPS took over the supervision of Eurojust at a crucial time – in 2020, the European Commission (EC) presented its Communication on the Digitalisation of Justice in the European Union[1]. One of the objectives set out in the EC's document is to further improve cross-border judicial cooperation between competent authorities at the European level. To this end, the EC announced that it is exploring ways to increase the availability of relevant machine-readable data produced by the judiciary, in order to establish trustworthy machine-learning AI solutions for interested stakeholders to use. Shortly after, in April 2021, the EC presented a proposal for an AI Regulation laying down harmonised rules for the EU, otherwise known as the Artificial Intelligence Act (AI Act)[2]. In both of these contexts, the EC stressed that any actions put in place must be in full compliance with the EU's fundamental rights, including the right to the protection of personal data. The AI Act would also designate the EDPS as the competent authority for the supervision of EUIs as they develop and use AI systems[3].

The use of AI tools in the area of justice may represent a high risk to the fundamental rights of individuals[4]. This is especially true with regard to AI systems that may be used to assist judicial authorities in factual and legal research, as well as in interpreting and applying the results of such research in a specific case. Such high risk is largely absent in cases where AI systems are used for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases, such as anonymisation/pseudonymisation of judicial decisions/documents or purely administrative tasks and allocation of resources. The formal views of the EDPS and of the European Data Protection Board (EDPB) on the new regulatory framework are expressed in their joint opinion issued in June 2021[5].

With this written contribution for Eurojust's 20th anniversary, we take this opportunity to reflect on some of the data protection issues stemming from the proposed AI rules on one hand, and the ongoing reform of Eurojust on the other.

Relationship between the data protection framework and AI rules

When speaking about AI, we usually start by reminding readers that a comprehensive European data protection framework, adopted on the basis of Article 16 TFEU, already exists. The data protection framework of Eurojust consists of the Data Protection Regulation for the EUIs (EUDPR)[6] and the specifying data protection provisions of the Eurojust Regulation.[7] While the Law Enforcement Directive (LED)[8] is not directly applicable to Eurojust, it determines the way in which national judicial authorities of Member States protect personal data for the purposes of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties.

Contrary to the European Public Prosecutor's Office and Europol, to which the EUDPR does not apply for the processing of operational personal data[9], the Eurojust data protection framework can be regarded as both clearer and more comprehensive. The EUDPR governs the processing of administrative personal data, and, together, its Chapter IX and the provisions of the Eurojust Regulation, constituting a *lex specialis* to the general rules, apply to the processing of operational personal data. We must stress the need for consistent interpretation and application of these rules – something that the text itself underlines[10]. It should be clearly stated that the existing data protection rules apply to the processing of personal data by Eurojust, whenever carried out wholly or partly by automated means, including possible processing by AI systems. There should be no doubt that the essential data protection requirements, derived from Article 8 of the EU Charter of Fundamental Rights, such as the principles of necessity, proportionality, accuracy, purpose limitation, data minimisation, integrity and confidentiality, continue to apply. Other obligations of the controller, such as data protection by design and by default, are also relevant. Whenever personal data is processed, data protection provisions apply. It should be clear that, when it comes to the processing of personal data, the new AI regulation would be without prejudice to the existing rules[11].

Human involvement

One of these rules deserves a special mention here. Article 77 of the EUDPR prohibits a 'decision based solely on automated processing', unless authorised by EU law as providing adequate safeguards – which should include at least the right to obtain human intervention from the controller. Such decisions (if authorised by law) shall not be based on sensitive data 'unless suitable measures to safeguard the data subjects' rights, freedom and legitimate interests are in place'. There is a clear requirement for specific safeguards to tackle the risks linked to the processing of sensitive data in automated processing used for decision-making.

To that end, controllers need to provide for human involvement in the processes where AI operates. The use of AI systems should involve systematic human intervention, evaluation and validation by expert staff. Human validation should be employed as an inherent step to ensure that the output of the systems is faultless. In the case that the automated results are assessed as faulty, the human intervention should provide feedback to be recorded and used for retraining the AI. How to best implement meaningful human involvement is certainly a topic for another article; here, we want only to stress the importance of such a safeguard, while being mindful that it is not the only factor to consider.

AI training and data minimisation

AI regulation discourse often seems to avoid the problem of potential conflict between AI development and the data minimisation principle. According to the conventional understanding of AI, data is an essential strategic resource and any meaningful progress in cutting-edge AI techniques requires large volumes of data, including personal data. Training of AI models relies on the data 'feeding' them. The more and better-quality data used, the better the AI tool is trained. AI developers are constantly seeking datasets that could improve the functioning of their creations. However, such an approach is in opposition to the principle of data minimisation. This fundamental principle is rarely considered when discussing AI regulation. However, it remains applicable to any processing of personal data. Designers and developers should therefore ask themselves whether it is really necessary to train a particular model on personal data. The data minimisation principle, combined with the principles of data protection by design and by default, are general requirements when using anonymous data if possible[12]. If the AI tool can be trained on anonymised datasets, collecting or injecting personal data in the training process should not take place. Current research demonstrates that AI is not synonymous with big data, and there are several other approaches that can be used in different small data settings[13].

Is AI a silver bullet?

We all know that digital transformation has profoundly changed people's lives in recent decades and will continue to do so. The use of AI in the public sector, including in the area of criminal justice and cross-border cooperation, is increasingly being explored. We understand there are high expectations regarding the possible benefits of these solutions; for instance, to help make judicial decisions machine readable, to simplify the reuse of case-law or simply to improve legal practitioners' advice to clients. Although AI can be used in process automation, it should not be seen as a universal solution to all problems and shortcomings. Even when the development of AI is delegated to a third party, the process of correctly developing an AI system demands the work and attention of people who know how the organisation works. It is a fallacy to believe that AI will, by itself, magically correct procedures that were already problematic.

While digital tools often contribute to the greater efficiency and effectiveness of today's judicial systems, it is crucial that their deployment should take into account the requirements to guarantee higher standards for the public justice service as well as the expectations and needs of the justice system's professionals and users. The use of digital technologies in the justice sector is highly sensitive and must therefore meet state-of-the-art standards with regard to information security and cyber security, and must fully comply with privacy and data protection legislation and with the standards upheld by the rule of law.

When discussing the use cases of AI models with representatives of law enforcement and of the judiciary, we are often given the impression that the principles of necessity and proportionality in particular are not sufficiently addressed. We believe that the development of machine-learning models needs to be driven by the proven ability of the model to fulfil a specific and legitimate purpose and not by the availability of the technology. In assessing necessity, EU entities should demonstrate that their purposes could not be accomplished in another reasonable way[14]. They should demonstrate a real need for AI to process personal data, how the processing effectively addresses this need and that the same purpose cannot be reasonably achieved with other, less invasive means. The main argument made in this context is that the growing volume of processed datasets can indeed be considered a starting point for the necessity assessment. This argument may provide a general reason for the use of AI to effectively carry out specific tasks entrusted to EUIs. Nevertheless, there are still elements that need to be added in order to complete the necessity assessment. Such assessment should explain and document why some AI models are preferred to others, to justify the selection of the least intrusive solution from a personal data perspective.

Possible use cases of AI systems for Eurojust

Given Eurojust's role as the EU hub for supporting and strengthening judicial cooperation between national authorities in charge of investigating and prosecuting serious crime, it seems that certain types of AI applications would fit this role better than others. For example, if we consider Eurojust as an agency that does not conduct its own investigations, tools for forensic analysis or visual biometric identification would not be at the top of the list, especially given the strong reservations around the intrusiveness of such means and the potential overlap with other actors, such as Europol.

However, there are other AI categories that seem highly relevant for cross-border judicial cooperation, such as various natural language processing (NLP) tools. These technologies are particularly useful for the processing of large-scale sets of unstructured data, commonly handled by judicial authorities. NLP technologies can support and facilitate Eurojust's main tasks by improving its internal processes; for example, these tools can be used for automated document processing, machine translation in cross-border cases, text summarisation or named-entity recognition.

Automated document processing

Considering that Eurojust is starting the process of designing and developing its new case management system, automated document processing (ADP) seems an obvious candidate for a use case[15]. ADP proves to be particularly valuable for processing high volumes of documents, especially for the classification, conversion and archiving of these documents in searchable formats. These types of AI systems can not only significantly reduce the need for manual document processing, but can also contribute to improving data accuracy and completeness. The conversion of paper-based formats into searchable documents is also the first step in exploring further deployment of other AI-driven tools, such as machine translation.

Automated translation

Overcoming language and communication difficulties between judicial authorities of the EU Member States was one of the driving forces behind the creation of Eurojust. It is also a strong argument for the application of AI in the context of cross-border cooperation in criminal justice. The need to communicate and analyse evidence in multiple languages is self-explanatory, particularly for joint investigative teams (JITs) supported by Eurojust[16]. Integrating automated translation tools into JITs' operations could significantly reduce the time spent on translation and make the evidence directly accessible to all team members; not to mention the reduction in costs for sworn translation, which would still be necessary for evidence to be admissible in court.

However, the specificity of cross-border judicial cooperation seems to be a problem when it comes to machine translation. Domain-specific legal language can pose a challenge to generic automated translation systems available on the market, as they are not reliable when distinguishing specific legal terminology from the generic language. To produce a high-quality translation, domain-specific terminology needs to be 'learned' and integrated into the AI tool. The research in this area is advanced and has generated promising results[17]. Nevertheless, domain-specific customisation would still require time and significant resources.

Automated summarisation systems

Another type of NLP tool to support cross-border criminal justice cooperation is text summarisation (summarisation systems). These tools prove to be particularly useful in applications where large amounts of information need to be processed in a limited amount of time. Summarisation systems facilitate the extracting of the most relevant information, significantly reducing the time needed to analyse large volumes of text, such as documentation seized in criminal investigations. Summarisation systems can also improve data classification and accessibility, especially in cases where processing by humans would take too long and where precision is not decisive.

Legal research

We turn now to another use case for NLP technologies: their use in legal research to facilitate the identification of case-relevant statutes, provisions and case-law. While this might be dispensable for research on the law of the EU Member States or non-EU countries posting Liaison Prosecutors to Eurojust (with Eurojust here fulfilling its role as a knowledge hub), there are instances where knowledge of foreign law is necessary for Eurojust to make informed decisions concerning data protection. We refer to the assessments of appropriate safeguards, provided for in Article 56 of the Eurojust Regulation. Knowledge about foreign data protection regulations applicable in the transfer of operational personal data to non-EU countries is an important element of Eurojust's assessment of existing data protection safeguards. This is a potential use case where AI technology could directly support the application of data protection provisions. Moreover, legal research supported by AI would not require the AI tool to process individuals' personal data. However, linguistic barriers might be a particular challenge in these situations, making this another case where automated translation could come in handy.

The AI Act and Eurojust's cooperation with third countries

Since we have already mentioned Eurojust transfers to third countries, allow us another digression on this point. Some of the solutions proposed by the AI Act might appear complicated when it comes to Eurojust's relations with external partners. The EC proposes to limit the scope of the AI Act with regard to international law enforcement and judicial cooperation. This would mean that the provisions of the draft AI Act, according to its Article 2(4), would not apply to public authorities in a third country or to international organisations, if these authorities or organisations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the EU, or with one or more EU Member State. In our view, Article 2(4) would not, in any way, limit the application of the AI Act to EUIs; only public authorities in third countries and relevant international organisations could 'benefit' from this proposed exception.

The practical application of such an exception in the Eurojust environment raises some questions. While the AI Act would be applicable to Eurojust as it develops or uses AI systems, does this exemption mean that it would not (formally) be applicable to third countries' Liaison Prosecutors operating at Eurojust? We feel this issue merits some further reflection in advance of the negotiations between legislators.

Prior assessment and data protection by design and by default

While the EDPS takes note of new and emerging ideas, it is not our intention, nor our role, to plead for these ideas to be put in place. Prior to the set-up of these technologies, authorities considering such applications should perform a legal and ethical assessment to take into account the impact and any possible risk to the fundamental rights and freedoms of individuals, as well as their ethical and legal implications. It is also important to conduct the testing and evaluation of these technologies to ensure that their performance meet the relevant standards, especially regarding data accuracy and bias.

The processing of personal data is often at the heart of AI technologies. At the same time, the data collected, processed and stored in judicial systems may be highly sensitive, revealing intimate details about individuals or even causing a threat to their lives. Giving access to this data for the purpose of training algorithms has to be considered with extreme caution and under very strict conditions. Training, testing and validation of machine-learning models with operational personal data and for their further use in the context of a specific Eurojust activity should not be carried out before a data protection impact assessment is done, according to Article 89 of the EUDPR. In addition, we stress that the responsibility of the controller goes beyond that: it starts with adequate project governance, which should take into account the principle of data protection by design throughout the conception and development of the AI tool and system in question. A data-protection compliant AI tool or system can be achieved once the following are in place: clear commitments to this principle in the key documents of the project; policies, processes and methodologies that consider data protection at each stage of the project; by identifying privacy and data protection stakeholders; by assigning roles and responsibilities regarding data protection; by working with competent individuals; and by properly documenting all of these steps. Furthermore, sets of business-level requirements on data protection and mechanisms to assess compliance of the outcome are needed. The controller also needs to put in place procedures for the identification and elimination of any bias in the data used to further train AI models, and to verify that the training data used does not cause discrimination. Processes to check the training or validation of data sets must be built and documented, and procedures allowing for regular monitoring of the models regarding biases and their readjustment or retraining must exist. These processes should include statistical checks on the input and output data.

Final remarks

From an EDPS perspective, we can clearly see the added value of AI. AI solutions can help complete tasks in a much faster and more cost-effective way, and can also be more accurate and precise than humans, if deployed correctly. At a time when nearly all judicial systems are facing a backlog of cases to process, the promises of efficiency that AI brings cannot be ignored. AI can also detect duplicated information in a reliable way, which contributes to data minimisation and helps to reduce personal data processing by effective anonymisation. If correctly put in place, AI may help to reach true equality and improve access to impartial and objective justice.

Nevertheless, we also see the associated risks. Algorithms are only as good as their programmers and the data they have been trained on. This leaves AI systems vulnerable to human error or historical bias. Gains in speed and efficiency can easily turn into disadvantages, if personal data is collected and processed in an immanently biased way. Lack of human oversight and monitoring mechanisms may have dire consequences for the fundamental rights of individuals, as well as their trust in judicial systems and in the EU mechanisms supporting them.

Finally, we see many actors in the field trying to be the first to seize the potential benefits of AI. There is a need for a coordinated approach at EU level when it comes to EUIs' development and use of AI systems to support law enforcement and judicial cooperation. You can count on the EDPS to play its part in the EU's coordinated approach to AI.

[1] COM(2020) 710 final; Communication of 2 December 2020 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Digitalisation of justice in the European Union – a toolbox of opportunities'

[2] COM(2021) 206 final; Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts..

[3] Article 2 and 3 of the draft AI Act.

[4] The proposed AI Act would explicitly qualify 'AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts' as a high-risk system subject to a particular legal regime (see Annex III, point 8 (a)).

[5] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021 (available on the EDPS's website).

[6] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, pp. 39–98.

[7] In particular, Chapter IV of the Eurojust Regulation.

[8] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data 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, pp. 89–131.

[9] Article 2(2) and 2(3) of the Regulation 2018/1725.

[10] Recital 29 of the Eurojust Regulation.

[11] With some notable exceptions, such as the list of prohibited AI practices in Article 5 of the AI Act.

[12] For more details on data protection by design as an enforceable legal obligation, see the EDPS Preliminary Opinion no. 5/2018 on Privacy by Design (available on the EDPS's website).

[13] Small Data's Big AI Potential (available on the *Center for Security and Emerging Technology*'s website).

[14] See also the EDPS Toolkit on Assessing the necessity of measures that limit the fundamental right to the protection of personal data, as well as the EDPS quick guide to necessity and proportionality (available on the EDPS's website)

[15] Cross-border Digital Criminal Justice, Final Report (pp. 160-162) (available on the *Publications Office of the European Union*'s website).

[16] COM(2021) 756 final; Analytical supporting document accompanying the proposal for the Regulation on the JIT collaboration platform (available on the *European Commission*'s website)

[17] See for instance the Connecting Europe Facility Digital programme (CEF Digital) with the eTranslation tool (available on the *European Commission*'s website).