# Ethical and Legal Risks of Algorithmic and AI Tools Developed to Fight Against Trafficking in Cultural Property in the RITHMS Project

Amara García Adán and María Ángeles Fuentes Loureiro

ECRIM, Faculty of Law, Universidade da Coruña, 15071 A Coruña, Spain
Correspondence: amara.garcia.adan@udc.es, maria.fuentes.loureiro@udc.es

DOI: *https://doi.org/10.17979/spudc.000024.51*

*Abstract*: Algorithmic technologies, big data and artificial intelligence have also disrupted the legal field. AI tools used in police investigations and in the judicial process stand out. The tools developed in the RITHMS project are aimed at combating the illegal trade in cultural goods. These tools facilitate the identification of criminal networks and their members. They are also useful for monitoring art markets, online auction sites and social networks to detect suspicious transactions. This poses ethical and legal challenges, requiring risk analysis and ensuring compliance with data protection, procedural and fundamental rights legislation. The aim is to address these challenges to ensure responsible use by competent authorities.

## 1 Introduction

The RITHMS project (Research and Innovation in Tackling the Illicit Trade of Cultural Goods through Multidisciplinary Science and Technology)[1] [2] was born out of the need, on the one hand, to understand the phenomenon of illicit trade in cultural goods and, on the other hand, to increase technological preparedness against the crime. RITHMS arises from the need to understand the functioning of markets for cultural goods. It is one of the least understood and supervised markets; there is still uncertainty in the provenance of objects, lack of traceability and poorly tracked transactions that contribute to an optimal scenario for crime. Thus, the project is aimed at solving the problems faced by Law Enforcement Agencies (LEAs) in dealing with this type of crime.

Experts widely acknowledge that the illicit trade in cultural property is no longer a localised phenomenon driven by a handful of individuals. On the contrary, it has become a lucrative source of income for criminal organisations that take advantage of the opportunities provided by online auctions and the visibility offered by social networks to further expand the already flourishing "grey market". This involves smuggling, theft and cross-border trade in valuable

[1] This paper has been prepared within the framework of the research project RITHMS – Research, Intelligence and Technology for Heritage and Market Security (GA 101073932) [HORIZON-CL3-2021-FCT-01-08]. Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

[2] Much of the information used in this article has been gathered from work on the above project, which will be publicly available on the RITHMS website. In particular, reference is made to Deliverable 1.1 on the Initial Legal Requirements, which is included in Work Package (WP) 1. On the other hand, Deliverable 7.1 on the Legal Framework is included in WP 7.

cultural and heritage property. This boom in transactions of illicitly obtained cultural property has been fuelled by the general lack of sound regulations governing this market, inconsistencies in national legislation and the inherent difficulties in tracing the origin of objects.

In response to this context, the RITHMS project advocates an interdisciplinary approach, driven by the international nature of this criminal activity and its intricate connections with other illicit networks and its connections with organised crime. The project aims to formulate a replicable strategy to effectively counter the challenges posed by the illicit trafficking of stolen or looted cultural property.

The RITHMS project aims to strengthen the operational capacity of police, customs and border authorities to deal with the increasingly organised and polycriminal nature of trafficking in cultural property through research, technological innovation, outreach and training. It is a collaborative effort aimed at enhancing the operational capabilities of law enforcement agencies to address the complex and evolving challenges posed by illicit trafficking in cultural property.

To do so, we must first come to understand the dynamics of the criminal phenomenon of illicit trafficking in cultural heritage. This research work is essential, as it will underpin the developing of digital technologies in the collection and processing of evidence to be used in court. On this basis, the consortium will develop an innovative digital platform to be used by LEAs. RITHMS platform will stand out for its interoperability and multi-functionality, allowing the identification, assessment and analysis of relationships between criminal and non-criminal actors. It will be based on Social Network Analysis (SNA) which allows mapping and analysis of social connections between individuals and groups of individuals by exploiting graph theory (RITHMS, n.d.). By outlining the networks involved in the illicit trafficking of cultural property and their possible evolution, the platform will improve the accessibility and accuracy of information available to LEAs. This tool will empower authorities in their efforts to combat illegal trade and better understand the dynamics driving these criminal groups.

Thus, RITHMS will equip LEAs with technological tools to increase their capacity to trace trafficking in cultural property and to prevent the emergence of organised crime networks through a technological platform developed and validated according to the needs and requirements of the professionals. To this end, it is necessary to the consortium will create a knowledge-base (in the form of multiple, structured datasets) related to the illicit heritage market and its actors, including: existing open datasets from LEAs, open sources (especially social media platforms), mobile network traffic datasets, satellite imagery, financial forensics and a database fed through custom-developed tracking software capable of detecting objects auctioned or sold directly online. Thus, based on this database, an algorithmic application capable of identifying the dynamics and actors of criminal networks involved in the trafficking of illicit goods will be created.

The development of this tool raises important legal questions. In order to use such a tool in the field of criminal law, whether at the investigative stage or in court, it is necessary to analyse the ethical and legal risks involved in the development and final use of the RITHMS platform. Data protection legislation, procedural law and, ultimately, fundamental rights, must be taken into account when developing such applications in order to avoid irregularities and infringements of rights and to ensure their legal validity.

## 2 Methodology

Within this project there are nineteen partners from eleven different countries including: Bosnia Herzegovina, Bulgaria, Croatia, Finland, Germany, Italy, Moldova, Romania, Spain, Switzerland and The Netherlands. The project coordinator is Dr. Arianna Traviglia from the Istituto Italiano di Tecnologia. The RITHMS consortium has been strategically assembled to ensure that it can effectively support exploitation and is aligned with an end-user approach. In particular, the consortium includes six police and border agencies, providing a deep understanding of end-user requirements. This will ensure that the technology developed is fit for purpose.

The Law Enforcement Agencies (LEAs) working with RITHMS will continue to be involved in the post-project phases, actively testing and providing real-time feedback to improve the platform. At the same time, industry partners will play a key role in the technical development of the platform, including data collection, satellite data integration, graph generation and AI advancements. In addition, research and technology organisations (RTOs) with expertise in technology transfer will provide strategic support by assessing market potential and identifying secondary market opportunities beyond crime-fighting applications.

The involvement of legal, ethical and policy partners (UDC, EEMA, HföD, CPT, EIM) will ensure that RITHMS complies with and contributes to European and international regulations, principles and standards. This involvement will also enable future collaboration, sharing of best practice and policy contributions., ii) concepts and iii) models that will guide the actions to be taken and the development of the technological deliverables, in particular the RITHMS Platform.

The core concept of RITHMS is based on a series of assumptions that include the widespread diffusion of intelligence-led policing as an organisational model for law enforcement. Such organisational models can greatly benefit from an automated intelligence tool based on SNA that provides actionable knowledge and information on complex and often transnational criminal networks. The information generated by the analysis of social networks involved in cultural heritage trafficking greatly benefits the effectiveness of investigations and prevention, allowing law enforcement agencies to direct their resources (human and technological) towards specific targets, where the reward is more relevant (such as effectively dismantling the criminal network or recovering assets).

The concepts that RITHMS will use during its lifetime revolve around SNA: an analytical tool that studies the links within social entities in a rigorous and quantitative way. It models social interactions through a graphical representation and can shed light on the relationships between actors (nodes) and on the flow of information, financial resources and goods through the network. Several modules will be able to feed the Platform with various data sources, merged into a correlation engine. AI models will also be used to implement the predictive capabilities of RITHMS, with a graph representation. Based on the above, the RITHMS methodology will be organised according to this structure: needs assessment and user-centred design; research on the nature of cultural heritage crime and the intersections between organised crime; development of an SNA-based platform and validation.

Regarding the work of the legal ethics team of the University of A Coruña, it begins with the completion of several studies on the initial legal requirements, the legal framework and some etichal issues. The study on the legal framework follows a methodology consisting of comparative and legal analysis techniques to analyse the qualitative data collected through the following means: - National reports on the six countries of the industry partners, five of which are EU Member States and one is not, and the six countries of the Consortium's law enforcement agency partners (LEAs), three of which are EU Member States and three of which are not. - Desk research to assess information published in the EU, internationally and in the countries under study.

As for the second study, the initial legal requirements, its methodology follows a requirements definition process. The requirements determination process usually consists of three stages (Pitts and Browne, 2007): information gathering, representation and verification. It is necessary to search for and analyse all useful sources to identify the elements that should guide the development of the system from the design phase. For this process, two perspectives can be used: on the one hand, the localising perspective, applicable to legal issues, which assumes that requirements are something that actually exist and simply need to be found. This perspective implies that the requirements are stable and recognisable. On the other hand, the constructionist perspective aims to create something new by combining identified elements in new ways.Compliance with these requirements will be monitored throughout the duration of the project and, in this case, will consist of respect for both rights and freedoms and legal provisions.

The legislative acts relevant to the project need to be identified and specific requirements extracted, in particular those stemming from the General Data Protection Regulation (hereinafter GDPR[3]) and the Law Enforcement Directive (LED [4] The detailed methods and approaches for analysing the EU and national legal frameworks were as follows:

A) Approach to analysing the EU legal framework: in this phase of the analysis we studied, through desk research, the relevant EU legislation. The analysis followed the approach described above as applied to international law, but also took into account the distinctive features of the EU legal system.

B) Approaching national legal frameworks: this research also analysed the legislations of the six EU and non-EU countries relevant to the use of the RITHMS platform in the end-user phase. The LEAs participating in the consortium were identified in order to balance the following criteria: i) participation of the countries (Bulgaria, Bosnia and Herzegovina, Spain, Italy, Moldova and the Netherlands); ii) presence of both police forces and border authorities; iii) relevance of the countries and their role in the illicit trafficking of cultural property; iv) presence of experienced partners with specialised units and others in the start-up phase.

The final step was to gather input and expertise from the consortium partners and project stakeholders to develop the initial version of the system requirements. An online questionnaire was used to collect information from the LEAs that will be involved in the use of the system. The legal requirements were then extracted from the information submitted by the Consortium's legal experts.

Since the specific characteristics of the multifaceted RITHMS platform and its components cannot be fully known in advance at the time of drafting the requirements, two corrective measures have been put in place to prevent the risk of impertinent requirements. The first measure is to ensure close interaction between partners with different expertise within the Consortium, in order to ensure that legal experts are aware of technology developments within the project, and that industrial partners are fully briefed on the practical consequences of changes in the legal framework. The second corrective measure is to involve end-users in the development of the system. End-users' views on their expectations regarding the project's results and the functioning of the platform will be taken into account throughout the project. During the co-creation phase, the views of the LEAs involved in the project and of the companies' ethics committees will be gathered.

## 3 Discussion

As we have already mentioned, developing a tool of these characteristics entails a series of ethical and legal risks. After analysing the project proposal, a series of ethical risks were identified that can be classified into three groups. Firstly, Internal AI risks, which are those inherent to AI technology. In the second place, Operational AI risks, which correspond to risks that emanate from the interaction of the technology with the real world and, in the third place, User risks, which are characterised by the risks that appear when the user applies the technology.

Regarding internal AI risks, i.e. inherent AI risks, opacity and lack of accountability emerge. This constitutes a risk in terms of the formation of algorithm black boxes. The lack of trans-

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[4] 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

parency about the functioning of the algorithm may lead to the potential incomprehensibility of automated decisions to human reasoning (Danaher, 2016) and, thus, to a lack of explainability and justification of the decisions taken, which is a fundamental requirement of European legal systems. Therefore, the use of these systems around police or judicial decisions should not undermine the ability to be able to explain decisions taken by public officials as their legitimacy depends on this.

In terms of operational AI risks, one of the first risks that appears is privacy interference. The very nature of the RITHMS platform, or similar platforms, has the risk of violating data protection law. This poses a very high risk in the development and use of the platform and will require privacy and data governance.

Data protection rights have been recognised for some time, with different levels of protection depending on whether the data is public or private. As mentioned, at the European Level, GDPR must be taken into account. In the specific context of criminal investigations within the European Union, the LED has established specific guidelines for the collection and analysis of data for the purpose of preventing, investigating, detecting or prosecuting criminal offences and ensuring public security. As a tool for crime investigation, all these provisions should be taken into account in the development of the RITHMS platform. However, it is important to remember that those rules constitute a minimum framework and that national rules may vary from country to country. It is therefore crucial to take into account the specificities of the countries in which the RITHMS platform is developed, tested and deployed.

Regarding data protection and privacy rights, we can highlight the risk that arises from the processing of data for investigative purposes that were not originally collected for that purpose. In the use a scraping technique, on which the RITHMS data collection is based, it is likely that the data were collected in the first place by private companies in the course of their business and are not related to crime. So there is a risk of using data for purposes other than those for which it was originally produced and stored. As the regulation of data collection is different depending on the purpose of data collection and processing, this entails the legal risk of the violation of the purpose limitation principle of Article 5(1)(b) GDPR. We should bear in mind that the misuse of such investigative technologies could disrupt law enforcement proceedings and affect the admissibility of evidence in court. For example, an abusive use of the platform as it can be used to identify any person of interest raises questions about the privacy of individuals and, in addition, this tool could start to be used for wider and wider purposes. Discimination and bias are also one of the risks identified. This risk is found in all three groups mentioned above. Discrimination can be found in how the target variable and the class labels are defined, in discrimination based on feature selection or in proxy discrimination which, in the appearance of neutrality, emerges as discrimination. Therefore, special attention should be paid to how data are collected and what kind of data are involved. If data are poorly labelled, inaccurate, incomplete or if it reflects human prejudices, then the AI model will reproduce those same biases (Surden, 2020)

Closely linked to the above is the timeless sequencing risk. AI needs to be trained with inputs, but those inputs belong to the past. The use of information in a sequenced and timeless way can lead AI to reiterate paradigms that are culturally, economically or legally outdated. This is a risk that raises the need for the information used as input to be subjected to a process of timing, i.e. adaptation to the present. Thus, we cannot fall into mathwashing, i.e. we cannot cling toto the false idea that an algorithm is free of bias, as it is assumed to be neutral and objective, but must seek control measures to minimise this risk. The use of such platforms may also lead to a possible violation of due process and fair trial guarantees (Quezada-Tavárez et al., 2021). This may result in the invalidity of certain evidence and lead to impunity for criminal actions for lack of lawful evidence.

First, it may lead to the inadmissibility of evidence obtained in violation of fundamental rights or without due proportionality. This is important because there are a number of legal standards that must be met for evidence to be admissible at trial, including procedural standards for obtaining evidence without violating rights. Otherwise, the evidence will not be

admitted at trial or will be declared invalid. And even if lawful evidence comes to light after the trial, the principle of ne bis in idem prevents the same individuals from being tried again for the same facts, even if lawful evidence subsequently comes to light.

On the other hand, the defendant's access to the information used for sentencing may be reduced with the use of technologies such RITHMS platform due to the algorithm opacity, and this infringes the principle of contradiction that governs criminal proceedings and thus the right of defence (Marquenie, 2019). A person who is accused has the right to know on what information his or her accusation is based, so if he or she is accused or convicted on the basis of a partially secret or incomprehensible algorithm, his or her right to defence would be violated (Virginia Foggo, 2020).

There may also be a violation of the right to the presumption of innocence. The principle of presumption of innocence requires that persons be presumed innocent until proven guilty according to law. Consequently, this principle is violated if a conviction is based on illegal or unlawful evidence, as it would result in a verdict without valid incriminating evidence. It is therefore essential to prevent evidence obtained during the police investigation phase from being obtained without due respect for the fundamental rights of the accused person during the collection of such evidence.

These risks of rights violations, among others, in the investigative process are exacerbated by the fact that many EU member states do not have specific regulations on intelligence-led policing and, consequently, the limits or requirements for such activity are not established. It should be borne in mind that the development of technological tools similar to RITHMS is relatively recent, so we should not be surprised by the lack of regulation in this regard. The EU and non-EU Member States that do have specific legislative provisions have mostly enacted them recently, but without considering the notion of tools using Big Data or Artificial Intelligence.

Therefore, for the time being, its use must be must be guided by the general rules of criminal procedure of each country. Finally, it is necessary to mention the Proposal for Regulation on Artificial Intelligence (the AI Act[5] ) which is expected to enter into force next year. This Act is structured in categories according to the risk presented by the system. There are four levels of risk in relation to AI practices: unacceptable risks; high risks; limited risks; minimal risks. The RITHMS platform would fit into the high risk level, which are not prohibited (unlike unacceptable risks) but are subject to a detailed certification regime.

The IA Act requires suppliers of high-risk IA systems to conduct a prior conformity assessment before placing them on the market. Suppliers must ensure that their systems comply with the "essential requirements" set out in Chapter 2 of Title III of the IA Act. They can then affix a CE marking on compliant systems, which can be freely imported and distributed throughout the EU. This includes data governance, i.e. rules on how input data sets should be designed and used, rules on the preparation of the data and the assessment of the formulation of relevant assumptions [about] the information that the data are supposed to measure and represent. In addition, these systems must be designed and developed in such a way that they can be 'effectively monitored by natural persons during the period that the AI system is in use, allowing the human supervisor to detect anomalies and to correctly interpret the results. If a high-risk system is operated by a "user" rather than the original provider - for example, a LEA buys and installs the RITHMS Consortium's platform - the allocation of responsibilities is very different in the Act than in the GDPR.

[5] European Commission. (2021). 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. COM/2021/206 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

## 4 Conclusion

For all these reasons, the tool developed in the framework of the RITHMS Project is a very interesting tool for combating trafficking in cultural goods. However, it is necessary to pay attention to all the requirements that these tools must meet in order not to violate the fundamental rights of citizens. This will require all partners to work together to provide the necessary expertise to develop this tool.

## Bibliography

J. Danaher. The threat of algocracy: Reality, resistance and accommodation. *Philosophy & Technology*, 3(29):245–268, 2016. An optional note.

T. Marquenie. The impact of predictive policing and law enforcement ai on human rights: The right to fair trial under pressure, 2019.

M. G. Pitts and G. J. Browne. Improving requirements elicitation: an empirical investigation of procedural prompts. *Information Systems Journal*, 17(1):89–110, 2007.

K. Quezada-Tavárez, P. Vogiatzoglou, and S. Royer. Legal challenges in bringing ai evidence to the criminal courtroom. *New Journal of European Criminal Law*, 12(4):531–551, 2021.

RITHMS. Rithms. https://rithms.eu/communication/press-kit/rithms-press-release/file, n.d. [Online; accessed 1-September-2023].

H. Surden. 719Ethics of AI in Law: Basic Questions. In *The Oxford Handbook of Ethics of AI*. Oxford University Press, 07 2020. ISBN 9780190067397.

J. V. Virginia Foggo. Artificial intelligence, due process, and criminal sentencing. *Michigan State Law Review*, pages 295–354, 2020. URL *https://core.ac.uk/download/pdf/327102171.pdf*.