RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0168 • articolo sottoposto a peer review • pubblicato in anteprima l'11 set. 2024

Pilar Martín Ríos

Predictive algorithms and criminal justice: expectations, challenges and a particular view of the Spanish VioGén system

The irruption in the field of the Administration of Justice of instruments linked to Artificial Intelligence and to the algorithms on which it is frequently based, is a well-known reality. In addressing this issue, some problems will inevitably need to be resolved, relating to access to justice, transparency or the impact of the digital divide. In this study, we will focus on the examination of AI in the Administration of Justice in general and, specifically, on its influence on criminal proceedings. Within this framework, we will also examine the emergence of the use of systems that, while employing algorithms, do not meet the criteria that allow them to be classified as AI. We will focus on the Spanish case, using the VioGén system as a paradigmatic example, although it is unavoidable to refer to the overall situation, given the global dimension of the analyzed phenomenon.

Criminal process – Artificial Intelligence – Predictive justice – Precautionary measures – VioGén

Algoritmi predittivi e giustizia penale: aspettative, sfide e una visione particolare del sistema spagnolo VioGén

L'irruzione nel campo dell'amministrazione della giustizia di strumenti legati all'intelligenza artificiale e agli algoritmi su cui spesso si basa è una realtà ben nota. Nell'affrontare questo tema, sarà inevitabile risolvere alcuni problemi legati all'accesso alla giustizia, alla trasparenza o all'impatto del digital divide. In questo studio ci concentreremo sull'esame dell'IA nell'amministrazione della giustizia in generale e, nello specifico, sulla sua influenza sui procedimenti penali. In questo contesto, esamineremo anche l'emergere dell'uso di sistemi che, pur impiegando algoritmi, non soddisfano i requisiti che consentono di classificarli come IA. Ci concentreremo sul caso spagnolo, utilizzando il sistema VioGén come esempio paradigmatico, anche se è inevitabile fare riferimento alla situazione generale, data la dimensione globale del fenomeno analizzato.

Processo penale – Intelligenza Artificiale – Giustizia predittiva – Misure cautelari – VioGén

The Author is Associate Professor of Procedural Law at the University of Seville (Spain)

Work carried out within the project *Transición digital de la Justicia*. Ref.TED2021-130078B-I00 (Spanish Ministry of Science and Innovation)

1. Methodological premises

The application of Artificial Intelligence (AI) and the use of algorithms in the Administration of Justice – particularly in the criminal field – has proven to be an invaluable tool in case management and decision making. In our paper we will go from the general to the particular, starting with the analysis of such techniques and tools in the Administration of Justice in general, to then descend to the criminal justice level and, within it, to do the same in relation to the precautionary protection. Within the latter, we will use an empirical-inductive approach to analyze the VioGén system by examining a Spanish case.

For this work we have used the logical method, both analytical and deductive[1]. We have also sought a critical and proactive approach, being the proposal of solutions our main pretension.

In terms of methodological techniques, jurisprudential analysis plays a crucial role in our study, without neglecting the due examination of numerous legal texts (Spanish Constitution, organic and ordinary laws, international treaties and European regulations), as well as abundant recent scientific doctrine.

2. Preliminary considerations: the emergence of Artificial Intelligence (AI) in the Administration of Justice

We cannot ignore the fact that modern justice tends to be, in a universal way, a "data-oriented" justice[2], so the competent judicial authorities will have to handle a high volume of data in their decision-making process. Undoubtedly, the availability of large amounts of information will require AI-based methods to manage it[3].

Although the implementation of technological tools facilitates the resolution of many of the problems that hinder the effectiveness of justice, it cannot be ignored that, at the same time, it has become the origin of other different ones. Precisely for this reason, having an adequate and sufficient regulation of its application and development is, more than ever, an unavoidable requirement.

Both the transparency and efficiency of the Administration of Justice would be enhanced by an adequate transition from analogue to digital. However, on occasions there has been a certain haste in the implementation of instruments, channels or techniques linked to new technologies, without

1. Martínez Montenegro 2023.
2. As stated by the Spanish Ministry of Justice. Also of particular interest is Cteaje 2022.
3. In Spain, for example, different regulatory initiatives have been developed in this regard. The project *Artificial Intelligence for the Efficiency of Justice* is a good illustration of this. Its aim is to adapt AI to advanced judicial analytics, improve the management and knowledge of data to apply it to processes, guide legislative policies through a better understanding of the impact of data associated with legal regulations, facilitate the automatic translation of rules and resolutions into the co-official languages of the State and implement a comprehensive open data policy in the Administration of Justice.

the accompaniment, in addition, of adequate training or investment of material or human resources. These objective limitations increase the reluctance of some legal operators in the face of the technification of Justice, which constitutes one of the main obstacles to its proper development.

Moreover, while it is still necessary to adapt the classic structures of law to the new demands arising from the technological revolution, it should not go to the extreme of thinking that it would be necessary to reformulate the General Theory of Law to find a specific legal fit for this new reality. In short, it is a matter of trying to anticipate this new, much more complex reality at the regulatory level, so that it is the law that imposes the guidelines on AI, and not vice versa[4].

It is an undeniable necessity to subject AI to legal standards that guarantee that its operation will respect the rights of others. The EU's regulatory efforts are heading in precisely this direction. In the European context, the 2019-2023 Action Plan on European e-Justice contemplates as one of its fundamental pieces the progress in the application of AI in the field of Justice, defining in a more appropriate way the digital implications in this area and specifying the role of AI in the analysis of judicial decisions.

For its part, the European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe, in the conviction that AI can contribute to improving the efficiency and quality of the work of the courts, adopted in 2019 the first European Ethical Charter on the use of AI systems in judicial administrations. To this end, it sets out some basic principles: respect for human rights, quality and security in the analysis and automated procedure of judicial decisions, transparency in the methodology used during judicial decision-making and the promotion of control exercised by users, who must be informed of their rights with respect to the solutions proposed through means based on AI. These will therefore be the premises from which we will start our study, analyzing to what extent the current development/implementation of AI in our environment respects these elementary premises.

In December 2023, the European Parliament and the Council of the EU – in response to a request from the European Commission in 2021 along the same lines[5] – reached a political agreement on the AI Act. Final text was published on 12 July 2024[6]. The AI Act shall apply from 2 August 2026, with some exceptions. It responds to a fundamental objective: to ensure that the AI systems used in the EU are safe and respect citizens' rights. In this line, a "risk-based" approach is followed: the higher the risk, the stricter the rules[7]. The EU AI Act is the first comprehensive legal framework on AI worldwide, although China (*General AI Regulatory Law*) and the USA (Executive Order Safe, *Secure and Trustworthy Development and use of AI*) have approved AI regulations in recent times (2023).

3. The case for Criminal Justice

3.1. General considerations

With regard, in particular, to its use in the field of Criminal Justice, as a part of a broader trend characterized by the increased use of forensic science and scientific procedures within it – in the belief that they can provide the judge with more objective, safe and controllable elements[8] –, the irruption of the AI has placed us in a scenario of uncertainty. Even if one wants to trust in the potential it offers, it is inevitable to be suspicious of what is still an unfathomable terrain.

Algorithms can have various functionalities in the context of criminal proceedings. Alongside a hypothetical – and unrealistic, in our opinion – gradual replacement of the judge by a "robot judge", there are more feasible uses which may be of some

4. Rodríguez Lainz 2023.
5. *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).
6. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
7. As stated in the EU AI Act.
8. Brighi 2016; Moscarini 2015.

relevance. Thus, for example, it facilitates the analysis of large amounts of data that may have evidentiary value in a process, and it does so quickly and efficiently.

Not even the profusion of rigorous scientific studies on this subject[9] manages to dispel all the doubts raised by the assumption of algorithm-based tools and resources in this field, that has even motivated the existence of an "algorithmic criminal justice" to be considered[10].

The question must be analyzed in the light of the necessary respect for the protection of procedural rights and guarantees and the principle of "electronic judicial security" in all its dimensions: authenticity, confidentiality, integrity, availability, traceability and preservation (art. 53.2 [Spanish] Law 18/2011 of July 5, 2011, regulating the use of information and communication technologies in the Administration of Justice).

From a more particular perspective, we could not argue that AI can collaborate with the defense in planning and developing their own strategies in the process. In fact, more and more law firms have various AI tools that allow, through massive data processing, both the calculation of the chances of success of a given claim and the identification of patterns in judging activity. Although these are utilities that are not yet widespread in Spain, in the United States AI is used to challenge juries and judges, as well as to question the impartiality of witnesses.

On the other hand, it should be noted that AI could even favour the interaction of vulnerable groups with the justice system. Undoubtedly, various technologies that use AI would serve to improve the accessibility to the process for those who have a physical or mental disability, or for those who do not know the language used in the proceedings. In this way, they could make the documents included in the case more accessible (through their reading or automatic translation, if necessary), facilitate access to judicial information and, at the same time, make communication with the parties possible (or simplify, as the case may be). To sum up, it would be possible to provide technological support that, compensating for its limitations, helps those who need it to be and act in the process in the best possible way.

AI is presented, in addition to the above, as a useful tool to support victims of crime. In particular, AI-powered chatbots and virtual assistants offer information and support in cases of gender-based violence, especially in cases where women – having normalized certain behaviors over time – do not identify with the role of victims. Both in these cases and in those in which there is a paralyzing fear of expressing the situations they suffer, the anonymity and support guaranteed by this type of chatbot make them allies of notable importance.

Along with these well-known functionalities, there are other applications that are based on AI technology that are not as widely used. This is the case of biometric programs that proceed to voice recognition through AI techniques, which have been used – again, in victimization linked to gender violence – to detect traits in the victim that allow the identification of criminal behaviors that have been committed against them[11]. Together with these uses, we will examine how it can contribute to the development of the criminal procedure itself, and how it can compromise its basic principles.

9. Martín Diz 2021; Nieva Fenoll 2018; Vallespín Pérez 2023.

10. Huq 2019; Barona Vilar 2021.

11. Due to its relevance, it is interesting to bring up the program led by the UNODC-INEGI Center of Excellence, in Mexico City, which uses AI to analyze the calls received by 911 and detect, in them, the presence of gender-based violence. With the technique used, based on natural language processing, the aim is to identify emotions in the voice of those women who, having contacted 911 for other types of issues, could be experiencing an episode of gender violence. In Andalusia (Spain), on the other hand, with the collaboration of the Andalusian Women's Institute, the project "Certainty of the voice" is being developed, which seeks to design a common voice pattern through the calls made by women to the health emergency number (061). Even if they have not claimed to be victims of abuse at any time, AI is used to analyze their words, the expressions used, the intonation, the rhythm, the pauses, the repetitions and even the silences that can be observed in those calls. In short, even the smallest detail that may reveal an emotion that is associated with suffering from a situation of victimization is taken care of.

3.2. Possible virtualities of police use of AI in criminal cases: detection, deduction and prediction

The involvement of AI in the criminal justice field cannot be examined without reference to its use by police forces. In our view, three possible virtualities can be identified in the use of AI in policing: detection, deduction and prediction. It is through this prism – the examination of AI in these three facets, which we believe can be identified – that we will approach this question.

As regards the first of these, AI contributes to the "detection" of certain circumstances. In particular, a system has been developed in Spain that allows the identification of false reports. Under the name "VeriPol", it is a system that, using natural language processing methods and a mathematical model, evaluates the probability of a complaint being false. It also makes it possible to identify patterns of behaviour, in such a way that it is able to determine which are the singularities that most distinguish false reports. In short, the aim is to elucidate the veracity of statements made by possible victims of crime. Apart from the fact that it does not require any information from the user, and is fully automatic, empirical experiments show that it is over 90% accurate, while expert police officers are over 75% accurate[12].

In 2014, a team of researchers from a Spanish and an Italian university developed this pioneering tool, which is based on examining the language used in a report to indicate the likelihood of it being true. It was created for cases of theft and robbery with violence and intimidation, due to the fact that it is in these areas where an increase in the number of simulated crimes has been detected in recent years.

From this analysis it can be concluded that true and false reports differ mainly in three main aspects: modus operandi of the aggression, morphosyntax of the report and amount of detail[13].

Continuing with the detection work, AI-based tools also help to detect the presence of certain individuals in particular places. This is particularly useful in the course of a criminal investigation and also at the police level, to allow for a massive policing. In this respect, AI makes it possible to analyze huge amounts of data, e.g., from video and audio recordings. It undoubtedly facilitates criminal investigation to a very considerable degree[14].

We find, in this respect, AI-based technology that enables facial recognition. Even though this and other biometric technologies are particularly risky, as highlighted by Murakami[15], its use is widespread in several areas[16]. It is significant that the proposed European Regulation referred to above, which is the result of the agreement reached in 2023, now contemplates something that it did not initially do: the possibility of remote, real-time biometric identification in public spaces, provided that it is carried out by law enforcement authorities and subject to certain safeguards[17].

In addition to these uses of mere detection or identification, AI facilitates, in a deductive way, the discovery of the alleged perpetrators of a criminal act. It provides information that is relevant to such deductive activity and does so, moreover, by providing standardized an data based guidance for case handlers to collect, examine and verify evidences[18]. The RACR system and the Patternizr tool, both used in the United States, are also highly significant[19]. In both cases, patterns are identified and, by establishing relationships between them, it is easier to determine the presumed perpetrators.

12. According to data from the Spanish Ministry of the Interior.
13. Alonso 2021.
14. García Sánchez 2022.
15. Murakami Wood 2006.
16. The control of transport and airports, in particular, although it is even being implemented in companies to facilitate payments.
17. This will only be possible for the commission of certain crimes, the prevention of real threats and the search for people suspected of the most serious crimes. On the other hand, indiscriminate tracking of facial images taken from the internet or CCTV is not allowed.
18. Cui 2019.
19. Alonso 2021.

Besides from that, in the field of crime prevention, the use of AI by the police is a reality that is growing exponentially, in the framework of what is known as predictive policing. The predictive tools (as CAS, Crime Anticipation System) make it possible to identify places where crime is most likely to be committed (the so-called crime heat maps, where the "hot spots" can be recognised). AI also allows these maps to be dynamic, real-time maps[20].

In other words, it will be sufficient to have data enough for the corresponding algorithm to yield information about the probability of a behaviour being carried out, as a mere statistical reflection, bearing in mind that the usefulness of predictive techniques will vary according to the crime in question[21]. Knowing this data undoubtedly helps to make patrolling more effective and results in a better distribution and use of material and human resources.

Regardless of the aforementioned, from a predictive point of view, there is a growing use of algorithms for the calculation of probabilities of different kinds (and not only in the field of policing, as we shall see). In general terms, we can define predictive analytics systems as the application of machine learning or deep learning capable of extracting patterns from historical data to predict future events or behaviours, giving a numerical value or score to the probability of a particular event happening, and suggesting actions to obtain more optimal results[22].

This would be the case, for example, with its possible use when determining the possibility of recidivism of an offender and, consequently, as an instrument for carrying out a prognosis for social reintegration and as a tool for assessing victim risk[23]. In our opinion, it should be, in any case, a support for the work of the judiciary and not a usurpation of it, since it takes on a different dimension when it ceases to be "just another instrument" and becomes the core of the judicial decision, as we will have occasion to explain. However, courts heavily weigh these models in their decisions[24]. COMPAS, in the United States, RISC, in Netherlands, or PSA (Public Safety Assessments), in the United Kingdom, are just a few examples.

The greater risk arises, in our view, when it comes to quantifying the probability that a given person will commit a crime, as in the case of the UK algorithm HART (Harm Assessment Risk Tool). It is even done to determine the possible serial criminal action of a person[25], through crime linking systems, such as Keycrime or Precobs software. Undoubtedly, the latter use presents greater problems in terms of acceptance. Precisely because of its importance, it will be the one that occupies our attention in the following sections.

3.3. AI and judicial activity: algorithms and the right of defense

In the following pages, we will analyse how the shift towards a justice system in which the algorithmic function plays a considerable role could affect the due respect for the right of defense. It is not a theoretical exercise, carried out on a hypothetical and future plane. Algorithms are already being used in the Administration of Justice, although they still do so on a small scale, in very specific areas, and have not even come close to reaching all the development of which they are capable.

In this regard, we must bear in mind the words of Paulesu[26], who wonders how the use of AI can be combined with respect for the table of values (constitutional and supranational) that characterises the fair process (equality of arms, personal freedom, right to defense, presumption of innocence, contradiction and impartiality of the judge). This is, of course, a considerable legal challenge, and must

20. Custers 2022.

21. CEPEJ 2019 states that there are crimes that are not so regular in nature, or that are simply characterised by the fact that their effects are produced in different locations. In these cases, the predictions that can be made will be less relevant.

22. García 2023.

23. The VioGén system is a clear example of this.

24. Custers 2022.

25. Basile 2019.

26. Paulesu 2023.

also be our starting point, the prism from which we approach our research: the needed balance between AI and the respect for these rights.

Let us start from the premise that all parties to the proceedings, including the accusers, must – as a manifestation of the right to obtain effective judicial protection – be guaranteed the exercise of their rights of defense. However, the limitations that may occur in the framework in which we now operate are perhaps most evident with regard to the subjects involved in a process. It is obvious that they must have an effective possibility of defending themselves, and this will depend, in practice, on respect for certain guarantees in the process.

Equality, which, as an inalienable principle of the process, must be verified throughout its development, is one of the main victims of an algorithmic criminal justice model. The so-called "digital divide" is particularly important in this area. It is undeniable that the imbalance of economic resources will translate into unequal access to certain AI systems, which could have a decisive impact on the future of a process. This difference will be particularly significant in civil proceedings, by virtue of the interplay of the dispositive principle. In criminal cases, it is expected that these techniques and remedies will be applied, *ex officio*, by the judge. This gap can also be seen in the unequal digital training of legal operators, which will lead to a deficient application of available AI resources.

For instance, reflect on the complexity of defending oneself against evidence and allegations that are primarily based on algorithmic systems, which are inaccessible to those affected by their procedural consequences. Furthermore, consider how our conception of the right to defense would shift if, in scenarios where the principle of opportunity is applied, negotiations over a potential conviction were conducted between a robot prosecutor and a robot defense attorney[27].

In order to ensure that the difference in status between the parties does not result in unequal access to justice and an impediment to the effective exercise of the rights of defense, it may be appropriate to adapt the benefits included in the benefit of legal aid to the new times and extend them to more current demands, such as the use of the latest AI technologies and access to techniques for the mass processing of legal aid.

This is not the only area in which equality could be compromised. AI systems can present biases – as is well-known from the *Loomis case*[28] –, which will be those of the individuals who configure the algorithms on which they are based. The prejudices and inequalities that are at its base will be predictably reflected in its outcome. For that reason, recital 71 of Regulation (EU) 2016/679 (Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) calls for the application of a principle of algorithmic non-discrimination, to avoid what is known as GIGO (garbage in, garbage out), that is, that the algorithm is built on data that is, in origin, discriminatory.

In addition, taking into account the difficulties inherent in any process of purging responsibilities that could result from the inadequate functioning of algorithms, it will be particularly complex to demand accountability in the event that a situation of injustice does occur.

Progressively, society is becoming aware that the exchange of data that takes place between large companies to draw profiles of potential customers must be subject to control and transparency. In the US, for example, the recent Algorithmic Accountability Act obliges large companies – provided that certain requirements are met – to audit their algorithms.

It seems understandable that similar clarity should be required when it comes to the creation of profiles or patterns that serve the fulfilment of police functions of crime prevention and detection. In the same way, value judgments must be made about the probability of recidivism of a subject. In any case, it is advisable to insist on the importance of preventing them from being based on *ab initio* discriminating algorithms. Otherwise, there would be a perpetuation of certain inequalities and prejudices that clearly need to be eradicated[29].

Transparency, in the end, is a basic condition for the proper exercise of the rights of defense. While this necessity is evident in any judicial pro-

27. Fernández Galarreta 2021.

28. On the *Ewert* case, similar to the *Loomis* case, see Giacomelli 2019; Vallespín Pérez 2022.

29. Villegas Delgado 2023.

cess, where every decision is documented and justified through "traditional" means, it becomes even more relevant when procedures or decision-making processes are based on the application of algorithms.

The problem lies not only in the scientific-technical complexity of the arguments that could be used to justify decisions based on mathematical formulas – the understanding of which will only be available to those with specific training in this regard[30] – but also in the publicity that is made of the technology used as the basis for them. An example of this is the software used, which should always be provided by public bodies and purchased in accordance with transparent tender conditions, subject to all the necessary control guarantees. It is certainly not a matter in which private initiative should be given an unrestricted entry, at the risk that interests other than the general ones will inspire the development of the algorithms that, in the end, will sustain decisions of enormous importance. It seems understandable that any judicial decision taken on the basis of an algorithm is subject to suspicion.

It is evident that nobody could attack with expectations of success what does not properly know. For this reason, basing decisions that have a certain relevance for the individual – as important as the adoption of a personal precautionary measure, for example, could be – on "black box" systems does not exactly contribute to diluting the reservations that exist in this regard[31].

While it is true that the mental mechanisms guiding a judge's decision-making are not fully understood, it is also true that this process is supported by at least two safeguards: recusal in cases where the judge's impartiality is questioned, and the requirement to provide reasoned judgments, which are subject to review through appeals. None of this is possible if we ignore the major premise: who, according to what criteria, developed the algorithms on which the decision is based.

But we must also consider a very different point of view: AI requires huge amounts of data for its operation, which feed the different algorithms on which a given system is based. On the basis that the confidentiality of the information in the proceedings is a requirement inherent in the same right of defense, it is necessary to draw clear limits that prevent sensitive information of the accused from nourishing this system, even though it could be useful for making predictions about their conduct.

Restrictions on publicity and transparency bring with them another important limitation, which now relates to the adversarial principle. It seems logical to deduce, from what has been stated, the impossibility of contradicting or refuting the results produced by an algorithm, result of a mathematical operation that is elusive and difficult to control. The possibility for the passive party to the proceedings to know and refute the evidence used against him will be clearly limited in such circumstances.

That the technology used at any stage of the procedure is known, accessible and verifiable is a requirement for its questionability. On the contrary, it leads us to a state of uncritical acceptance of the dictates of AI that will lead, in addition, to a situation of absolute defenselessness, to a true tyranny of the algorithm.

In our opinion, the use of algorithms designed ad hoc can facilitate – but not replace, since this is a barrier that we consider insurmountable – the work of the judge. It would be, in other words, an additional tool to obtain the precise information to decide in conscience.

In any case, it is essential that law enforcement and judicial authorities are always able to separate themselves from this interpretation, avoiding the potentially serious consequences that derive from an absolute adherence to the algorithm. As highlighted in the European Parliament Resolution 2020/2016 on artificial intelligence in criminal law and its use by law enforcement and judicial authorities in criminal matters of 6 October 2021, placing excessive reliance on the apparently objective and scientific nature of AI tools, which ignores the possibility that their results may be incorrect, incomplete, irrelevant or discriminatory, brings with it not inconsiderable risks.

30. Živković–Ducato 2023.

31. Cotino Hueso 2017; Donati 2020; González Álvarez–Santos Hermoso–Camacho Collados 2020; Pérez Estrada 2019; San Miguel Caso 2021; Simón Castellano 2021.

In this sense, we endorse, point by point, the following reflection of Judge Del Moral: «never, at least in the field of criminal justice (another thing is the civil sphere, in which the dispositive principle opens other doors), should we dispense with the primacy and protagonism of the human factor, of the judge who makes the decision. There are variables that a machine, AI, cannot provide. Judicial decisions emanating from a robot may be accurate. But justice is not the same as accuracy. We only approach Justice (without achieving it, but without renouncing that aspiration) through human decisions. That brings with it the potential for errors. But a robotic justice, entrusted to AI, would constitute a justice, perhaps without errors, but dehumanized (in the pejorative sense of the word). In short, it would not be justice»[32].

Since, in any case, the final decision will have to be taken by the judge – in that conception that we defend of the algorithm as a support, not as a substitute – it would be expected, in the scenario we describe, that it would be the judicial reasoning that would be discussed by the person affected by the measure, and not the operation of the computer program used, which would require a technical-scientific knowledge superior to that of the average citizen. The problem will arise if this reasoning is limited to being a reference to the result offered by the algorithm, automatically accepted and assumed as its own. In order to prevent the use of any algorithmic support system from infringing the rights of the defense, it will be necessary for it to be accompanied by a threefold requirement: human control of the operation, the possibility of departing from the suggested result and an exhaustive justification of why one way or the other is being taken. Any mere statement of reasons by reference, in view of the risks involved, should be expressly prohibited[33].

4. Particularizing the study: the algorithmization of the adoption of precautionary measures

4.1. Initial considerations

Without leaving the field of criminal justice, we will focus our attention on a very sensitive issue: making a prediction of a person's criminal tendency on the basis of mathematical formulas. Although judicial decision-making linked to the consideration of possible future behaviour is not new in our criminal prosecution[34], it would be different if AI techniques were used to make prognoses of dangerousness in an attempt to justify the adoption of pre-criminal measures or even the classification of citizens according to their criminal propensity. The application of these expert systems for predictive purposes in the judicial determination process is encompassed within what is known as Judicial Artificial Intelligence (JIA), whose subtype, Risk Assessment Artificial Intelligence (RVAI), is particularly noteworthy[35].

It is undeniable that the criminal justice system sometimes resorts to predictive judgements. Both in the adoption of security measures in criminal proceedings and in the application of social reintegration prognoses in the execution phase of sentences, value judgements are made.

Whether or not an algorithmic program is used for this purpose, there is no doubt that the application of a security measure is always caused by the realization of a previous forecast. In this case, its adoption is not based on the idea of guilt, but takes into account, among other aspects, the dangerousness of the subject, which must be proven within the process and may be subject to contradiction.

But what is the basis of such a judgment of dangerousness? Sometimes it is related to the very pathological states that led to the assessment of non-imputability or semi-imputability; in others, it follows from the very nature of the fact. In any case, and this is the most relevant thing, these are

32. Del Moral 2023.

33. In the same way, see the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (Brussels 8 April 2019 COM(2019) 168), *Building Trust in Human-Centric Artificial Intelligence* and the *Guidelines for Trusted AI developed by the High Level Expert Group on AI*.

34. Quattrocolo 2020.

35. García 2023.

objectively appreciable circumstances, since the security measures are based on the criminal dangerousness of the subject on whom they are imposed, externalized in the commission of an act foreseen as a crime.

The prognosis of future behavior that reveals the probability of committing new crimes is made to depend, apart from the nature and circumstances of the act, on "the personal circumstances of the subject", which could complicate this interpretation. Despite this, an examination of practice leads us to conclude that even in these cases, objective or "objectifiable" factual notes, such as the mental state or the medical-psychiatric history of the accused, are considered to be "personal circumstances". In other words, with a view to the imposition of a security measure, psychological examinations are not carried out to assess a possible inclination to crime. Nor is there the use of algorithmic programs to determine it.

As regards what happens at the stage of execution of the sentence imposed, it cannot be denied that reports are drawn up which do identify a certain tendency to commit offences and which serve as the basis for the preparation of a prognosis of recidivism. In practice, this type of data is used to make a prognosis for the social reintegration of convicted persons and to decide whether they should be entitled to prison benefits or access to the third degree or parole. However, there are two points to bear in mind regarding this possibility: firstly, these reports are prepared by experts, integrated into multidisciplinary teams with extensive training and experience. Therefore, mathematical programs that rely on algorithms are not used. Secondly, these are convicted persons, who no longer enjoy the presumption of innocence, so there would be no qualms about alluding to their dangerousness or risk of recidivism.

Having established the above, we must address what happens in another particular area of criminal prosecution: precautionary protection. Predictive justice, which is based on the application of algorithms, finds – at least from a theoretical point of view – a particularly favourable field in the possible adoption of precautionary measures. Such adoption is, in fact, based on the making of judgments of probability. In criminal proceedings, in particular, the imposition of pre-trial detention – configured, as we know, as the most restrictive personal precautionary measure – depends on the assessment of at least one of the so-called "three risks": flight, repeat offence or destruction, alteration or concealment of evidence. In that regard, it must not be forgotten that the assessment of a risk really requires the drawing up of a prognosis for a specific person.

It is clear that, when adopting precautionary measures, the risk of recidivism and re-victimization is taken into account. All this, translated into the language we are now using, is intimately linked to that dangerousness to which we have already referred, so it is necessary to ask ourselves on what basis the judge's judgment is based on this possibility of criminal repetition that then leads him to impose a precautionary measure. Of course, it does so on the basis of objective data, derived from the very nature and circumstances of the act allegedly committed. No objection can be raised in that regard.

Greater problems would arise, however, if, along with this type of information, the judge were to assess another series of characteristics linked, as we said, to the personality or character of the subject in question, from which it could be deduced – that is what is really risky (above all, because the presumption of innocence still operates, at this moment, in full force) – a "tendency to crime".

In other words, we would only have to accept that a precautionary measure is due to the assessment of the risk of recidivism when this could be objectively founded, as is the case with the prognosis of danger that precedes the imposition of a security measure, as has been said. If its adoption were made in view of the personality of the person (by analysing, for example, the websites visited, the media consulted, the blogs participated in, the tweets published or, in general, the opinions expressed on the Internet), we consider that the presumption of innocence of the person who has to bear it would be compromised. We would also be entering the dangerous terrain of offender-based criminal law. As Paulesu points up[36], it is necessary to avoid "juxtaposing the assessment of personality and the assessment of responsibility".

And, in assessing that risk of recidivism, would it be admissible to obtain that information from

36. Paulesu 2023.

some algorithmic system? Leaving aside the undeniable difficulty implicit in any effort to anticipate human behavior, we must analyze whether making precautionary measures dependent on predictions of algorithmic origin would help to facilitate their application or, on the contrary, would pose an additional problem. There are those who argue, in this regard, that this prognosis is more easily admissible when it is made by a person (even if it is made on the basis of vague and difficult to verify criteria), and more criticizable when it is made by a machine[37].

It is not hidden from us that, in fact, the use of algorithmic predictive systems aimed at the application of a precautionary measure is a reality in various legal systems. However, difficulties are observed both in the way these systems are designed and in the way they are developed: first of all, because trying to determine the existence of such a tendency, before a conviction is handed down, implies, as we said, a clear compromise of the right to the presumption of innocence; secondly, because in these cases it is essential to know what kind of information will be used to make such a value judgment. Regardless of the general criticisms about the obscure functioning of algorithms (and the recurrent mention of the *black box system*)[38], where could the algorithmic programs used obtain information[39] on a hypothetical tendency to commit a crime? It should be borne in mind that, in criminal proceedings – at least in Spain[40] – judicial expert opinions are only carried out to determine the imputability/non-imputability of the accused.

4.2. The Spanish case: VioGén

In Spain, the fight against gender-based violence shows remarkable singularities in the matter at hand. Although the assessment of any "inclination to crime" (which today may be based on psychological examinations and, tomorrow, may consist of genetic or epigenetic analyses), should not be included in the declaratory phase of the criminal process, where the presumption of innocence still applies, it is true that in the field of gender-based violence – surely due to the frequent revictimization that accompanies this phenomenon and the need to put a stop to it – the Comprehensive Forensic Assessment Units (UVFI)[41] make recidivism prognoses of the aggressor taking into account, among other data, his personality. This prediction is made, of course, in a "traditional" way, without resorting to AI systems, through the joint work of professionals in medicine, psychology and forensic social work. The fact that the psychological profile of the alleged aggressor is drawn up by expert multidisciplinary teams can be accepted as necessary in the fight against such a major problem.

However, we are more concerned about the fact that, in order to make these probability judgments to which we alluded, ad hoc computer programs are used. For years, in order to prevent gender-based violence, State security forces have resorted to the "police risk assessment" protocol (known as VPR), which is the main core of the VioGén system[42]. It is the police who reflect in their report the percentage of risk of revictimization, as estimated by the VioGén system. This interpretation is made automatically, based on the algorithmic reading of the

37. Contissa–Lasagni–Sartor 2019.

38. In our view, the lack of knowledge about the functioning of algorithmic activity can give rise to two extreme and opposing positions: the uncritical acceptance of the conclusions reached, as we have seen, or the general distrust of the answers offered. In this regard, as some authors point out (Contissa–Lasagni–Sartor 2019), it is necessary to move from an approach based on "data fundamentalism" to one based on informed trust.

39. It could certainly be provided as a party expert, but not constitute a judicial expert.

40. It is interesting to note that article 220.2 of the Italian Code of Criminal Procedure expressly prohibits (except in the execution phase) psychological examinations of the accused in an attempt to determine the possible existence of a tendency to commit crimes. Quattrocolo 2019 highlights how in many States in North America and Australia, predictive software based on psycho-criminal assessments has been used for some time.

41. Integrated into the Institutes of Legal Medicine and Forensic Sciences, by virtue of Organic Law 1/2004, of 28 December, on Comprehensive Protection Measures against Gender Violence.

42. Implemented by Instruction 4/2019 of the Secretary of State for Security, which establishes a new protocol for the police assessment of the level of risk of gender-based violence, the management of the safety of victims and the monitoring of cases through the comprehensive monitoring system for gender-based violence cases.

information provided. This, in turn, is obtained from the responses incorporated into a questionnaire completed by the police, which includes thirty-nine different risk indicators.

It should be noted, however, that it is a predictive system based on algorithms but it is not, strictly speaking, AI[43], since this instrument does not use algorithms that "learn" from data processing[44]. In short, it uses statistical models to infer the risk that a victim may run, based on a set of indicators that have been previously determined.

Of course, as will be seen, the system described is very different from the risk assessment carried out in the UVFI and the prognosis that, as we have seen, is made in the execution phase of the criminal process, both of which are characterized by the involvement of multidisciplinary teams of experts. If, even in such cases, it is risky to entrust the judicial decision to an estimated calculation of probabilities (taking into account the unpredictability of human nature), our skepticism about VioGén seems understandable[45].

We have insisted on the idea that, in relation to any prediction that is made, it is particularly important to pay attention to the data on which it is based. And it is at this point that, we believe, another important objection to VioGén should be raised: some of the information contained in the questionnaire that "feeds" the algorithms on which the prediction is based is, in our opinion, especially delicate. We are referring, in particular, to questions that allude to the existence of jealousy or a desire for control on the part of the partner, clear indicators of a certain personality, if not even of a true psychopathology. Worse still is to ask directly, as is done in the VPR form, about the existence of a mental or psychiatric disorder of the alleged offender. That these notes are taken into consideration only by a computer program, after having been supplied by the alleged victim of the crime (therefore, inevitably, subjectively), and that this results in the assessment of a certain level of risk may also lead to the imposition of measures restricting the liberty of the alleged aggressor is hardly acceptable to us. Bearing in mind, moreover, that this diagnosis of dangerousness cannot be contradicted, the right of defense is, in our opinion, as compromised as the presumption of innocence.

The fact that VioGén does not seem to us – at least, as it is configured – to be an adequate channel for the decision on the adoption of measures does not mean, either, that we deny the effectiveness that algorithmic systems, in general, can have in the field of precautionary protection, where they could play a supporting role in the work of the judge, as a particularly useful assessment tool that should not be underestimated. We acknowledge that any initiative in this regard should not only respect the previously mentioned considerations[46], but also meet an additional requirement: there must be oversight of the types of data utilized. This will support the integrity of algorithmic predictions. In no case do we believe that it is admissible for the application of these programmes to entail the entry into our criminal system of considerations that concern the psychological sphere of the passive subject of the process and that may contribute to forming a criterion about his greater or lesser inclination to crime. Not only should they have no place – for the sake of the presumption of innocence – in the declaratory phase of criminal proceedings, but they should never be assessed exclusively by a computer program. Although VioGén confines itself to making a statistical interpretation of the data provided, without further analysis, it is, in our opinion, a first step in a direction from which we must flee. The algorithmic elaboration of psychological profiling, already present in other areas, must be radically excluded from our justice system.

43. Presno Linera 2023; Pérez Marín 2023.

44. González Cabanes–Díaz Díaz 2023.

45. The Council of Europe's Group of Experts on Combating Violence against Women and Domestic Violence (GREVIO) evaluated the VioGén system in their 2020 Report on the implementation of the Istanbul Convention in Spain and noted that a significant percentage of women killed by their partners or ex-partners were considered as low-risk cases by the VioGén, which raises the question of whether breaches are taken "too lightly".

46. Consequently, the last word should be left to a person, there should be room for contradiction between the parties, there should be transparency and publicity of the system used and the judicial motivation should be exhaustive.

5. Discussion

The readers of this paper will learn how algorithms – usually, but not always, linked to AI – are acquiring an increasing importance in the framework of the Administration of Justice, they will know the favorable aspects that this entails and, also, they will be aware of the problems that their use may have in a very specific framework: the criminal precautionary protection. It is in this area where the greatest criticisms of the work will be found. We have used as a paradigmatic example of the above a case that is well known in Spain: the VioGén system. This system involves the application of certain algorithms by the police, in order to determine the risk of repetition of a crime by a detainee arrested for gender violence. As all this translates into the adoption of one or another criminal precautionary measure, it is a clear example of predictive justice.

In short, we have proposed a study that goes from the general (the critical examination of the entry of algorithms into the Administration of Justice) to the particular (their entry into the criminal justice system – at the hands of two of its protagonists: the police and the judges – and, more specifically, in the so-called precautionary measures).

The results obtained in our research are in line with numerous criticisms that – more generally – have been made by the scientific doctrine. Although there are studies that address the impact that the entry of these modern instruments into the Administration of Justice may have on procedural rights and guarantees, the originality of our work lies in having applied these general considerations to a specific scenario: the area of precautionary protection and, more specifically, the VioGén system, about which considerable reticence has been expressed and justified.

It has not been our intention to undertake a comprehensive and exhaustive examination of how the different precautionary measures can be affected, to a lesser or greater extent, by the information that algorithms can provide (which could undoubtedly be the subject of further studies). We have preferred to focus, instead, on the specific examination of what is happening in this regard in the field of gender violence in Spain. As is well known, this is a particularly problematic (and widespread) issue in our country, making the examination of this case especially representative. In our opinion, the way in which the VioGén system has been developed (especially taking into account the nature of the specific items to be completed), gives rise to significant problems. To this must be added the difficulties already present in any predictive justice system, as we have exposed.

6. Conclusions

Technology is a considerable and increasingly important part of our lives. It is a subject that, without being new, never abandons its relevance. Leaving aside its usefulness as an instrument in almost all spheres of our daily lives (provided that it is properly managed), it would be unfair to deny the wide range of opportunities that, in particular, it offers in the field of law.

From a general perspective, it is undeniable that the application of technology to the process results in accelerated processing, reduced time, and a notable saving of resources. It makes it possible to work with greater efficiency than human efficiency – which is not necessarily linked to effectiveness, as we well know –, which is a remarkable feature in the current state of congestion in the Administration of Justice. Also starting from the perspective of the omnipresent Sustainable Development Goals (especially goal number 16, linked to the promotion of peace, justice and strong institutions), AI could be understood as a particularly valuable resource. In other words, its use for handling such a large amount of data allows us to save time and effort in tasks that, traditionally, have been carried out in a more "artisanal" way. As we have already had occasion to highlight, it is important to insist that these resources should, in any case, be available to all parties to the proceedings, avoiding the inequalities that would arise if only large law firms had access to them.

Regardless of whether algorithms are associated with AI, it is important to recognize that their implementation within the field of the Administration of Justice involves a commitment to safeguarding fundamental rights and guarantees. In this paper we have focused on how the right of defense – and its diverse, multiple, manifestations – are affected by this, could be considered, algorithmic drift, which finds in the so-called "predictive justice" its most striking manifestation.

Assuming all of the above, one of the biggest obstacles to the peaceful acceptance of these new techniques and procedures lies in the way they are

designed and the obscurantism that surrounds them, which makes it extremely difficult to contradict any "algorithmic claim". The lack of knowledge of the functioning of such algorithms on the part of the citizen, which prevents questioning not only their mere creation but also the selection that – unavoidable – underlies the information from which they are nourished, brings with it the risk of their incontestability. We must not forget that in our model of criminal procedure there is a system of free evaluation of evidence that is diametrically distant from the possible consideration of the data provided by these algorithms as weighted evidence. Nor should the presumption of the veracity of algorithmic readings prevail, which would result in a de facto shift of the burden of proof to the accused and, consequently, in an unacceptable compromise of the rights of defense. Human control over the operation of the algorithm will be as necessary as the possibility of deviate from the solution it proposes. The judicial statement of reasons for their action will also be essential.

The lack of knowledge of multiple facets relating to the creation and operation of such algorithms limits – it seems beyond doubt – the effective exercise of the rights of defense. Not only will it be impossible to confront a decision (precautionary or otherwise) that is based on an algorithmic prediction of uncertain origin and operability – which is a clear violation of the principle of contradiction – but the very filing of appeals against it would be meaningless. The right to effective judicial protection would, in short, be seriously affected. It would not be unreasonable to venture, given the circumstances, that the famous *Loomis* case will be only the first of many.

An important part of our attention has been drawn to the examination of VioGén, as a paradigmatic example of a system based on predictive algorithms. In this sense, it is not only the data or the information used by the system – which, as we said, has some characteristics of psychopathological tests – that concerns us; it is also the way in which the system is set up, the training of those who have to assess the result it produces and the absence of expert supervision before the result obtained is passed on to the judge. We must reiterate this point: it is essential to avoid basing the adoption of a measure (whether precautionary or definitive) on forecasts that consider a hypothetical personal predisposition to commit a crime, particularly when such forecasts are the automatic outcome of an algorithmic application that utilizes data potentially indicative of certain personality traits, including psychopathological ones.

In light of the above, it is crucial to continue advancing in the development of fundamental requirements that underpin a rational and proportionate use of algorithms, particularly within the framework of criminal justice.

References

S. Barona Vilar (2021), *Algoritmización del derecho y de la justicia. De la inteligencia artificial a la Smart Justice*, Tirant lo Blanch, 2021

F. Basile (2019), *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in "Diritto Penale e Uomo", 2019

R. Brighi (2016), *Su statuto epistemologico e consolidamento tecnico-giuridico dell'informatica forense*, in "Anales de la Facultad de Derecho", Universidad de La Laguna, 2016, n. 33

CEPEJ (European Commission for the Efficiency of Justice) (2019), *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, 2019

Cteaje (Comité Técnico Estatal de la Administración Judicial Electrónica) (2022), *Manifiesto por un espacio público de datos en el ámbito de justicia*, 2022

G. Contissa, G. Lasagni, G. Sartor (2019), *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in "Diritto di Internet", 2019, n. 4

L. Cotino Hueso (2017), *Big Data e Inteligencia Artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales*, in "Dilemata", 2017, n. 24

Y. Cui (2019), *Artificial Intelligence and Judicial Modernization,* Springer, 2019

B.H.M. Custers (2022), *AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law*, in B.H.M. Custers, E. Fosch Villaronga (eds.), "Law and Artificial Intelligence", Springer, 2022

A. Del Moral García (2023), *Inteligencia artificial y justicia penal*, in "I Simposio Justicia y derecho en Datos", Ministerio de Justicia 2023

F. Donati (2020), *Intelligenza Artificiale e Giustizia*, in "Rivista AIC", 2020, n. 1

F.J. Fernández Galarreta (2021), *Derecho de defensa e inteligencia artificial. Reflexión crítica acerca de la repercusión de la inteligencia artificial en la profesión de abogado*, in A.I. Pérez Machío, J.L. De la Cuesta Arzamendi (dirs.), "Contra la política criminal de tolerancia cero", Aranzadi, 2021

M.D. García Sánchez (2023), *El necesario balance entre la heurística algorítmica y judicial como garantía de los derechos procesales del justiciable; hacia una inteligencia artificial explicable*, in P. Martín Ríos, C. Villegas Delgado (dirs.), "La tecnología y la inteligencia artificial al servicio del proceso", Colex, 2023

M.D. García Sánchez (2022), *Big brother ¿Ciencia ficción o realidad?*, in "Ius et Scientia", 2022, n. 8

L. Giacomelli (2019), *Big brother is «gendering» you. Il diritto antidiscriminatorio alla prova dell'intelligenza artificiale: quale tutela per il corpo digitale?*, in "BioLaw Journal – Rivista di BioDiritto", 2019, n. 2

J.L. González Álvarez, J. Santos Hermoso, M. Camacho Collados (2020), *Policía predictiva en España: aplicación y retos futuros*, in "Behavior & Law Journal", 2020, n. 6

F. González Cabanes, N. Díaz Díaz (2023), *¿Qué es la Inteligencia Artificial?*, in E. Gamero Casado, F. Pérez Guerrero (dir./coord.), "Inteligencia artificial y sector público. Retos, límites y medios", Tirant lo Blanch, 2023

A.Z. Huq (2019), *Racial Equity in Algorithmic Criminal Justice*, in "Duke Law Journal", vol. 68, 2019, n. 6

F. Martín Diz (2021), *Herramientas de inteligencia artificial y adecuación en el ámbito del proceso judicial*, in L. Bujosa Vadell (dir.), "Derecho procesal: retos y transformaciones", Atelier, 2021

I. Martínez Montenegro (2023), *Sobre los métodos de la investigación jurídica*, in "Revista chilena de Derecho y Ciencia política", vol. 14, 2023, n. 1

P. Moscarini (2015), *Lo statuto della "prova scientifica" nel processo penale*, in "Diritto Penale e Processo", 2015, n. 6

D. Murakami Wood (ed.) (2006), *A Report on the Surveillance Society*, September 2006

J. Nieva Fenoll (2018), *Inteligencia Artificial y proceso judicial*, Marcial Pons, 2018

P.P. Paulesu (2023), *Inteligencia Artificial y proceso penal italiano: una panorámica*, in P. Martín Ríos, C. Villegas Delgado (dirs.), "La tecnología y la inteligencia artificial al servicio del proceso", Colex, 2023

M.J. Pérez Estrada (2019), *El uso de algoritmos en el proceso penal y el derecho a un proceso con todas las garantías*, in S. Barona Vilar (dir.), "Claves de la Justicia Penal. Feminización, Inteligencia Artificial, Supranacionalidad y Seguridad", Tirant lo Blanch, 2019

M.Á. Pérez Marín (2023), *Violencia de género y algoritmización: la justa medida del sistema VioGén*, in D. Vallespín Pérez (dir.), "Algoritmización de la justicia penal", Juruá, 2023

M.A. Presno Linera (2023), *Policía predictiva y prevención de la violencia de género: el sistema VioGén*, in "Revista de Internet, Derecho y Política", 2023, n. 39

S. Quattrocolo (2020), *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Springer, 2020

S. Quattrocolo (2019), *Equo processo penale e sfide della società algoritmica*, in "BioLaw Journal. Rivista di BioDiritto", 2019, n. 1

J.L. Rodríguez Lainz (2023), *Prólogo*, in P. Martín Ríos, C. Villegas Delgado (dirs.), "La tecnología y la inteligencia artificial al servicio del proceso", Colex, 2023

C. San Miguel Caso (2021), *La aplicación de la Inteligencia Artificial en el proceso: ¿un nuevo reto para las garantías procesales?* , in "Ius et Scientia", 2021, n. 7

P. Simón Castellano (2021), *Inteligencia artificial y Administración de Justicia: ¿Quo vadis, justitia?*, in "Revista de Internet, Derecho y Política", 2021, n. 33

D. Vallespín Pérez (2023), *Inteligencia Artificial y Proceso: eficiencia vs. garantías*, Juruá, 2023

D. Vallespín Pérez (2022), *Intelligenza Artificiale e valutazione delle prove nel processo civile spagnolo e italiano*, in "Revista General de Derecho Procesal", 2022, n. 57

C. Villegas Delgado (2023), *Gobernanza algorítmica, ética de la inteligencia artificial y estado (algorítmico) de derecho. Retos para el jurista en la era digital*, in D. Vallespín Pérez (dir.), "Inteligencia Artificial y Proceso: eficiencia vs garantías", Juruá, 2023

P. Živković, R. Ducato (2023), *Algorithmic discrimination: a blueprint for a legal análisis*, EU and Comparative Law Issues and Challenges Series (ECLIC), 2023, n. 7