

THE RIGHT TO DIGITAL COMMUNICATION OF PERSONS DEPRIVED OF LIBERTY: FROM ABSOLUTE PROHIBITION TO INTELLIGENT CONTROL

Angela M. ATANASIU ^(*)

Abstract

The digital transformation of society has profoundly altered the social content of communication, work, education, and family relationships, without the penitentiary enforcement regime undergoing an equivalent normative adaptation. At present, persons deprived of liberty benefit from limited forms of telephone communication and, in certain restricted situations, from online communications; however, the general prohibition on the use of mobile phones and other telecommunication devices continues to reflect a normative logic specific to the analog era. In a context in which digital communication has become the ordinary infrastructure of social, professional, and educational life, maintaining an absolute prohibition raises questions concerning the proportionality of the restriction and its compatibility with the reintegrative purpose of punishment. This paper examines the right to communication of persons deprived of liberty from the perspective of the digital transformation of society and argues for the necessity of a reconceptualization of the penitentiary enforcement regime applicable to communications. The analysis begins with the domestic legal framework governing telephone conversations and online communications and highlights its principal dysfunctions: unequal legal treatment among different categories of persons deprived of liberty, the insufficient nature of the existing facilities, and the lack of a genuine correlation between penitentiary security and the need to maintain family and social ties. The paper argues that the appropriate solution does not lie in maintaining absolute prohibition, but rather in transitioning toward a model of intelligent control, in which the regulated use of digital communications is permitted within predetermined limits, under technological supervision and effective human oversight. Such an approach makes it possible to reconcile penitentiary order, the protection of fundamental rights, and the contemporary requirements of social reintegration.

Keywords: *digital communication, persons deprived of liberty, execution of sentences, intelligent control, social reintegration.*

1. Introduction

The execution of sentences and custodial measures is one of the fields in which the gap between social transformation and normative reaction is becoming increasingly visible. While, traditionally, discussions concerning detention were centered on physical isolation, institutional discipline, and the restriction of the exercise of certain rights, contemporary reality

requires a shift in perspective: social life itself has moved, to a significant extent, into the digital sphere. Communication with family, access to information, continuation of professional training, participation in educational activities, administrative relations, and even the exercise of basic forms of personal autonomy currently presuppose technologically mediated interactions.

It is well established that online communication is more effective than

^(*) Judge, Bucharest 3rd District First Instance Court– Criminal Section (e-mail: angela.athanasiu@gmail.com).

traditional telephone contact and may provide greater opportunities for improving family relationships for persons deprived of liberty presenting a high degree of vulnerability or special needs¹ and yet, the legal provisions governing the execution of sentences have failed to keep pace with the technological revolution that has shifted society into the digital world, marking a profound transition from the coin-operated telephone to the smart device capable of responding instantly to biometric interaction and image-based recognition.

Nevertheless, the legal provisions governing the execution of sentences continue, to a large extent, to reflect a normative logic insufficiently adapted to contemporary technological transformations. While society has undergone a profound transformation, moving from rudimentary forms of telecommunication to intelligent and hyperconnected digital infrastructures, the legal regime applicable to persons deprived of liberty has remained predominantly structured around mechanisms specific to an outdated technological paradigm.

In this context, the issue of the right to communication of persons deprived of liberty can no longer be analyzed exclusively by reference to traditional telephone conversations or correspondence in the classical sense. Digital communication no longer represents a mere technological convenience, but rather one of the ordinary infrastructures of social life. Consequently, the near-total exclusion of persons deprived of liberty from this environment no longer produces merely an ancillary limitation of private life, but may affect the very possibility of genuine reintegration into a profoundly digitalized society.

The subject matter of this paper lies at the intersection of penitentiary enforcement law, the protection of fundamental rights, and the adaptation of legal institutions to technological transformation. The starting point of the analysis is the observation that the current legal regime governing communications in detention largely preserves a philosophy of prohibition and controlled exception. Persons deprived of liberty may benefit from certain regulated forms of contact with the outside world; however, the use of telecommunication devices in the contemporary sense remains, as a rule, prohibited. Although this normative solution may be historically explicable, it is becoming increasingly difficult to justify from the perspective of proportionality and the purpose of punishment.

This paper seeks to demonstrate that the transformation of the social environment also requires a transformation of the penitentiary enforcement paradigm. The issue is not one of replacing penitentiary order with unconditional digital freedom, but rather of identifying a legal model capable of reconciling institutional security with the preservation of meaningful family, social, and educational ties. In this regard, the analysis supports the transition from absolute prohibition toward a model of intelligent control, based on limited authorization, technological filtering, and effective human oversight.

2. Digital Communication and the Transformation of the Social Content of Reintegration

The digital transformation of society has profoundly altered the social content of communication, work, education, and family

¹ Ioan Chiș, Alexandru Bogdan Chiș, *Executarea sancțiunilor penale, Curs universitar, ed. a II-a revizuită și adăugită*, Universul Juridic Publishing House, Bucharest, 2021, p. 680.

relationships, such that effective participation in social life increasingly presupposes technologically mediated interactions. At present, social life itself has significantly shifted into the digital sphere, and digital communication can no longer be understood as a mere technological convenience, but rather as one of the ordinary infrastructures of social existence. Under these conditions, the reintegration of persons deprived of liberty can no longer be conceived exclusively in traditional terms, by reference to the restoration of social ties in a physical sense or to mere compliance with the rules of social coexistence, but must also be correlated with the possibility of readaptation to a profoundly digitalized social environment.

Thus, the digital transformation of society has altered not only the instruments of communication, but also the very structure of social relations and the concrete mechanisms through which individuals participate in community life. Family life, professional integration, access to education, relations with public authorities, and the exercise of personal autonomy are today deeply dependent upon digital infrastructures and upon the individual's capacity to use technological tools for communication and interaction. Under these circumstances, the social reintegration of persons deprived of liberty can no longer be analyzed exclusively by reference to their readaptation to traditional norms of social coexistence, but must also be assessed from the perspective of their genuine capacity for reinsertion into a profoundly technologized social environment.

From this perspective, the execution of custodial sentences cannot remain isolated from the structural transformations produced within society through digitalization. If the purpose of punishment is to prepare the convicted person for reintegration into a functional social environment, then ignoring

the digital dimension of contemporary existence risks transforming the execution of punishment into a mechanism of adaptation to an already outdated social reality. In other words, reintegration can no longer be effectively achieved outside the technological reality into which the individual will return following the execution of the criminal sanction.

In this context, the near-complete exclusion of persons deprived of liberty from the sphere of digital communications may produce effects that go beyond the traditional restriction of the exercise of certain rights. Digital isolation risks generating a new form of penitentiary marginalization, characterized by the inability of the convicted person to maintain genuine contact with contemporary social mechanisms. Persons deprived of liberty are excluded not only physically from the community, but also functionally from the digital environment that currently structures essential social relations. Indirectly, this rupture may affect the continuity of family relationships, access to education and vocational training, as well as the possibility of developing skills necessary for subsequent social reintegration.

Moreover, it must be observed that maintaining an almost absolute separation between the convicted person and the digital environment creates an increasingly evident tension with the preventive-educational and reintegrative purpose of the execution of sentences. Insofar as contemporary society functions through digital mechanisms of communication, work, and social organization, the progressive adaptation of the convicted person to these realities becomes an integral part of the reintegration process. A penitentiary system that ignores this transformation risks accentuating the phenomenon of desocialization and amplifying the difficulties of readaptation following release.

From this perspective, the issue of controlled access to digital communications can no longer be reduced exclusively to the classical opposition between liberty and penitentiary security. In reality, the discussion concerns the manner in which the penitentiary enforcement system understands the need to redefine the relationship between control, reintegration, and institutional adaptation to the technological transformations of contemporary society.

3. The Current Legal Regime Governing the Use of Telecommunication Devices

The current legal regime governing the use of telecommunication devices within the penitentiary environment continues, to a large extent, to reflect an enforcement philosophy specific to the analog era. The prevailing normative model is structured around the logic of general prohibition and direct physical control, within which contact between persons deprived of liberty and the outside world is permitted only in strictly limited, predetermined, and institutionalized forms. Such a conception was historically justified by the necessity of maintaining penitentiary order and by the difficulty of exercising effective control over communications carried out outside infrastructures directly administered by the authorities.

However, the technological transformation of contemporary society has significantly altered the relationship between communication, control, and security. Whereas, in the past, the unrestricted use of telecommunication devices entailed risks that were difficult for penitentiary administrations to manage, the development of current technological mechanisms of monitoring, filtering, and traceability now allows for the configuration of forms of

control significantly more sophisticated than mere absolute prohibition. Under these conditions, the persistence of an enforcement model constructed almost exclusively around the exclusion of digital communications risks reflecting not so much an objective necessity of security, but rather the inertia of a normative paradigm insufficiently adapted to technological transformation.

From this perspective, the incompatibility between the current structure of enforcement norms and the reality of a profoundly digitalized society becomes increasingly evident. Digital communication no longer represents an exceptional or marginal activity, but rather one of the ordinary means through which individuals exercise their family, social, professional, and educational lives. Consequently, the near-total exclusion of persons deprived of liberty from this environment produces effects that go beyond the mere limitation of a technological advantage and may affect the very capacity for reintegration into a social environment structured around digital interactions.

Traditionally, penitentiary control has been conceived predominantly as a form of physical control: restriction of movement, supervision of direct contacts, and limitation of access to certain objects or spaces. Technological evolution, however, now makes possible a transition toward forms of intelligent control based not exclusively on prohibition, but on differentiated supervision, digital filtering, and traceability of use. Within this model, technology does not eliminate institutional control, but transforms it from an absolute material control into a functional and adaptive form of control, capable of managing concrete risks without completely excluding the convicted person from the digital sphere.

This conceptual transformation must also be analyzed in light of recent European

regulations concerning artificial intelligence and the use of digital systems impacting fundamental rights. Thus, the European Union Artificial Intelligence Act (AI Act) classifies certain systems used in the fields of law enforcement and justice as high-risk systems, subject to strict requirements regarding transparency, human oversight, and proportionality control. Although the use of digital surveillance mechanisms in the execution of sentences may pursue legitimate objectives of security and prevention, such mechanisms cannot operate in the absence of legal safeguards capable of preventing the excessive automation of restrictions on rights.

In this regard, the principle of human oversight acquires essential importance. The use of digital instruments for monitoring or filtering communications cannot lead to the replacement of effective human control through automated decisions. The intervention of penitentiary authorities and the possibility of individualized assessment must remain central elements of the enforcement process. Technology may function as a support tool for identifying risks, managing differentiated access, or ensuring the traceability of communications; however, decisions concerning the restriction of the exercise of rights must remain subject to human control and proportionality criteria.

Consequently, the fundamental issue is not whether the penitentiary system should exercise control over digital communications, but rather the manner in which such control may be exercised in a way compatible with the contemporary requirements of the protection of fundamental rights and social reintegration.

4. The Limits of Absolute Prohibition

The analysis of the limits of absolute prohibition regarding the use of telecommunication devices by persons deprived of liberty must be carried out in relation to the requirements of fundamental rights and, in particular, to the standards developed in the case law of the European Court of Human Rights (ECHR) concerning Article 8 of the Convention. Although detention inevitably entails restrictions upon the exercise of certain rights and freedoms, the Court has consistently held that convicted persons continue to benefit from the protection of the Convention, and that interferences with private life and correspondence must remain compatible with the principle of proportionality and with the legitimate aims pursued by the penitentiary administration.

In this field, the requirement of proportionality acquires particular relevance. Not every measure restricting communications is incompatible with fundamental rights, since maintaining institutional security and preventing genuine risks constitute legitimate objectives of the execution of sentences. The problem arises, however, when the restriction acquires a generalized, undifferentiated, and almost absolute character, irrespective of the concrete situation of the convicted person, his or her conduct, the nature of the identified risks, or the purpose pursued through the execution of the sanction.

From this perspective, the principal difficulty of the current normative model lies not in the existence of control over digital communications, but in its uniform and disproportionate nature. An enforcement system constructed almost exclusively upon absolute prohibition tends to ignore the necessity of individualized execution and transforms restriction into an autonomous

rule, relatively detached from the concrete assessment of risks and of genuine reintegration needs. Yet, the individualization of the execution of punishment presupposes precisely the adaptation of restrictive measures to the profile of the convicted person, his or her conduct, and the legitimate objectives pursued by the penitentiary administration.

Moreover, it must be observed that the progressive transformation of society into a profoundly digitalized space also alters the practical significance of exclusion from digital communications. Whereas, in a previous social context, limiting access to certain technological means could have had an ancillary character, today such restrictions risk producing far deeper effects upon the private, family, and social life of the convicted person. Digital communication currently represents one of the ordinary means of maintaining family relationships, accessing education, participating in professional activities, and exercising personal autonomy. Under these circumstances, near-total exclusion from the digital sphere may lead to the emergence of a genuine form of indirect social exclusion.

This evolution requires a clear distinction between legitimate penitentiary security and excessive restriction of the exercise of rights. The necessity of preventing unlawful activities, protecting institutional order, or avoiding risks related to penitentiary security cannot be disputed. Nevertheless, the mere existence of potential risks does not automatically justify maintaining an absolute and uniform prohibition applicable to all persons deprived of liberty, regardless of the particularities of their individual situations. In a state governed by the rule of law, restrictions on the exercise of rights must remain necessary, adequate, and proportionate to the aim pursued, rather than functioning as the

autonomous expression of an exclusively security-oriented logic.

In reality, maintaining an almost complete separation between the convicted person and the digital universe risks entering into structural contradiction with the very reintegrative purpose of the execution of sentences. If contemporary society functions through digital mechanisms of communication and social organization, then the prolonged exclusion of the convicted person from this environment may amplify difficulties of readaptation and intensify the process of penitentiary marginalization. From this perspective, the central issue is not whether penitentiary authorities should exercise control over digital communications, but whether the current model of absolute prohibition still constitutes a solution compatible with the contemporary requirements of proportionality and social reintegration.

5. From Absolute Prohibition to Intelligent Control

Overcoming the model of absolute prohibition requires the configuration of a new type of penitentiary enforcement paradigm, founded not upon the generalized exclusion of digital communications, but upon their controlled and intelligent use. Within this framework, technology no longer appears exclusively as a source of risk to penitentiary order, but also as an instrument capable of reconciling institutional security, the protection of fundamental rights, and the reintegrative purpose of the execution of sentences. The central issue is not the elimination of control, but rather its transformation into a differentiated, proportionate, and risk-adapted mechanism.

In reality, the digital transformation of the execution of sentences reflects a deeper tension between two contemporary paradigms of criminal justice: the logic of

predictive justice and the requirements of restorative justice. The development of algorithmic risk-assessment mechanisms and digital monitoring infrastructures encourages the emergence of an enforcement model oriented toward the anticipation of behaviors, the probabilistic management of risks, and the enhancement of institutional control efficiency. Within this framework, technology enables the identification of behavioral patterns and supports the configuration of differentiated supervision mechanisms based on predictive assessments.

In this regard, modern approaches to contemporary criminal policy pursue the implementation of restorative justice, defined by criminologist Tony F. Marshall as a form of justice grounded in responsibility, restoration, and social reintegration. According to him, restorative justice is, in essence, a process through which all parties involved in a particular offense come together in order collectively to determine how the consequences of the offense and its future implications should be addressed.²

This differentiated approach does not amount to a denial of the humanistic values underlying restorative justice; on the contrary, it represents a condition for its credibility and sustainability. The humanization of criminal law cannot be achieved through diminishing the State's capacity to protect life, physical integrity, and personal security, but rather through a careful and contextualized balance between rehabilitation and legitimate coercion.

Thus emerges the concept of predictive justice, which defines a new fundamental

principle of the judicial process: 'a principle of sincerity on the part of the judge, who should strive to offer litigants a new perspective, free from prejudice and from any predictive pressure'.³

In this context, predictive justice constitutes a deeply unsettling subject. On the one hand, it offers a promise of security and certainty, which may appear reassuring in the face of what is commonly referred to as legal uncertainty. On the other hand, however, the prospect of replacing human beings with machines is inevitably disturbing and may ultimately represent the very negation of justice itself.⁴

Nevertheless, the execution of sentences cannot be reduced exclusively to a logic of prediction and algorithmic control. The reintegrative purpose of criminal sanctions presupposes the preservation of a profoundly human dimension within the enforcement process, centered on accountability, the reconstruction of social relationships, and the progressive reintegration of the convicted person into the community. From this perspective, restorative justice cannot be replaced by automated risk-management mechanisms, since social reintegration involves elements that exceed the capacity of technology to operate solely on the basis of statistical correlations and predictive behaviors.

Consequently, the use of intelligent control mechanisms must be integrated into an enforcement model capable of avoiding the transformation of the convicted person into a mere object of algorithmic assessment. Technology may contribute to the individualization of the execution of

² Tony F. Marshall, *Restorative Justice: An Overview*, Kindle Edition, Coventry Lord Mayor's Committee for Peace & Reconciliation, Coventry City Council, United Kingdom, 2018, p. 3.

³ Antoine Garapon, Jean Lassègue, *Justice Digitale: Révolution Graphique et Rupture Anthropologique*, Presses Universitaires de France (PUF), Paris, 2018, p. 259.

⁴ See, in this regard, *La Justice Prédictive*, Actes Du Colloque du 12 Février 2018 organisé par L'ordre Des Avocats au Conseil d'état et À La Cour De Cassation à l'occasion de son bicentenaire en partenariat avec L'Université Paris-Dauphine PSL, Paris, Dalloz, 2018.

sentences and to the reduction of concrete risks; however, it cannot substitute the relational and restorative dimension of criminal justice. For this reason, artificial intelligence must remain a support tool for penitentiary administration, rather than an autonomous mechanism for decision-making concerning the enforcement trajectory of the convicted person.

Such a reconceptualization may be achieved through the development of an integrated digital enforcement infrastructure, built upon the principles of an Artificial Intelligent Penal Enforcement System (AIPES), within which technology functions as a support tool for the penitentiary administration, without substituting human decision-making. Within this framework, the use of digital communications by persons deprived of liberty would no longer be governed exclusively by the logic of total prohibition, but rather by mechanisms of gradual access, differentiated monitoring, and individualized control.

Within such a model, access to digital communications could be configured according to objective and verifiable criteria: the category of the enforcement regime, the conduct of the convicted person, the identified risks, the level of penitentiary trust, and the purpose of the activities carried out. Thus, the system would no longer operate on the basis of a rigid opposition between total access and absolute prohibition, but rather according to an adaptive logic, capable of distinguishing between different degrees of risk and different enforcement needs.

From a technological perspective, intelligent control presupposes the use of mechanisms of algorithmic filtering, digital traceability, and functional monitoring of communications. Concretely, technology

could allow the restriction of access to certain applications or platforms, the identification of behaviors considered incompatible with penitentiary rules, the verification of communication traceability, and the automatic signaling of potential risks to the penitentiary administration. Nevertheless, the function of such systems must not be confused with the autonomous exercise of decision-making power.

In this field, one of the most important conceptual limits concerns the relationship between artificial intelligence and human authority. Technology must not decide, but rather assist the penitentiary administration in the exercise of its duties. The role of digital systems is not to substitute individualized analysis or human judgment, but to provide additional tools for risk management, the organization of control, and the individualization of the execution of sentences. Consequently, any restrictive measure concerning access to digital communications must remain the result of effective human intervention and of a concrete assessment of the individual situation.

This idea reflects the necessity of maintaining meaningful human intervention within the enforcement process, in a context in which it has been argued that 'the secret is to keep humans involved in the decision-making loop—to use AI as an assistance tool, not as a crutch upon which we become dependent.'⁵

Moreover, the use of intelligent supervision mechanisms may contribute to overcoming the structural limits of exclusively physical control. Unlike the traditional model, predominantly based on prohibition and isolation, intelligent control allows for the exercise of continuous and differentiated supervision without

⁵ Ethan Mollick, *Co-inteligență, Cum să trăiești și să muncești cu AI*, Publica Publishing House, Bucharest, 2025, p. 68.

completely eliminating digital contact with the outside world. In this regard, technology may function as an instrument for reducing enforcement-related risks, without transforming the convicted person into an individual excluded from the digital social infrastructure.

Viewed from this perspective, predictive justice is not conceived as a mechanism of subjugation, but rather as one that encourages creation and even interaction. Prediction cannot bind or constrain legal professionals; it cannot constitute the basis of a decision, but it possesses the capacity to stimulate inquiry and to assist in the search for a solution hoped to be more equitable.⁶

In reality, the true stake of such a transformation does not lie in the excessive digitalization of the execution of sentences, but rather in adapting the penitentiary enforcement system to the actual structure of contemporary society. In a social environment increasingly organized through digital platforms and technologized communications, maintaining an enforcement model built exclusively upon the logic of exclusion risks becoming incompatible with the very purpose of social reintegration. From this perspective, intelligent control does not represent a weakening of penitentiary security, but rather a reorganization thereof within a more flexible, differentiated, and rule-of-law-compatible framework.

The governance of an Artificial Intelligent Penal Enforcement System (AIPES) presupposes a clear delimitation of competences among the actors involved, such that the activities of data collection, processing, and analysis remain distinct from the exercise of decision-making powers,

which must belong exclusively to the competent judicial and enforcement authorities. From this perspective, the integration of artificial intelligence into the execution of sentences cannot lead to the transfer of legal responsibility to autonomous algorithmic systems.

Accordingly, it becomes necessary to limit the delegation of penitentiary enforcement decisions to automated mechanisms. Artificial intelligence may be used particularly in fields characterized by large volumes of information, high complexity, and difficulties in rapidly identifying correlations relevant to penitentiary administration. In this context, intelligent systems may function as support instruments for data analysis, risk assessment, and the organization of enforcement control, without substituting the individualized legal assessment carried out by the human decision-maker.

Human beings are particularly skilled at recognizing new objects and understanding their purpose. Traditionally, when AI systems encounter something new for which they have not been trained to recognize, they may experience difficulties in classifying that object in the same manner as a human being would. However, a new artificial intelligence method known as 'one-shot learning' is beginning to address this limitation.⁷

Even though recent developments in the field of artificial intelligence allow for the emergence of increasingly sophisticated mechanisms of processing and adaptation to new situations, these technological advancements do not justify the elimination of human intervention from the decision-making process. The capacity of technology to identify patterns and operate upon large

⁶ Jean Francois Burgelin, *Sur le rôle de l'expert*, v. J. Sainte-Rose, « *Le juge face à la science* », in *Principes de justice. Mélanges en l'honneur de Jean Francois Burgelin*, Dalloz, Paris, 2008, p. 345.

⁷ Nigel Toon, *How AI Thinks: How We Built It, How It Can Help Us, and How We Can Control It*, Transworld Publishers, Penguin Random House, London, 2024, p. 70.

volumes of data does not equate to the ability to exercise the legal and moral judgments specific to the execution of sentences.

According to Ethan Mollick, when information is transmitted to AI systems, most contemporary large language models do not learn directly from those data, since they are not part of the model's pre-training process, which has generally been completed long beforehand. Nevertheless, the data uploaded may subsequently be used in future training sessions or for fine-tuning the model being used.⁸

Consequently, the integration of artificial intelligence into the enforcement system must remain subordinated to the principle of exclusive human responsibility for decisions concerning the execution of criminal sanctions. The role of artificial intelligence may be consultative, technical, and informative; however, the decision concerning the restriction of rights, the individualization of the enforcement regime, or the assessment of the convicted person's conduct must always belong to the competent authorities.

6. The Conditions for the Legitimacy of Intelligent Control

The legitimacy of a model of intelligent control concerning the digital communications of persons deprived of liberty depends upon the existence of legal and technological safeguards capable of preventing the digitalization of the execution of sentences from being transformed into an autonomous mechanism for restricting fundamental rights. In the absence of such limits, the use of surveillance and monitoring technologies risks leading not to a legitimate enhancement of the execution of sentences,

but rather to the emergence of forms of excessive control incompatible with the requirements of the rule of law.

From this perspective, recent developments in European law concerning artificial intelligence are of essential relevance. The European Union Artificial Intelligence Act (AI Act) classifies systems used in the fields of law enforcement, justice, and the management of activities impacting fundamental rights as high-risk systems. Such classification entails the obligation to comply with strict standards concerning transparency, human oversight, traceability of operations, and the possibility of verifying the functioning of the systems employed.

The necessity of maintaining effective human control over intelligent surveillance mechanisms becomes all the more important in the context of contemporary debates regarding the risk of the autonomization of systems based on artificial intelligence.

As Yuval Noah Harari warns, we are in danger of losing control over our own future⁹, in the context of the emergence of an informational network governed by the decisions of a non-human intelligence, potentially capable of functioning independently of human intervention. Although this perspective has the merit of highlighting the genuine risks associated with the excessive delegation of decision-making to autonomous algorithmic systems, we consider that such a vision tends to absolutize the technological potential of artificial intelligence and to underestimate the role of the legal, institutional, and ethical framework within which it is integrated.

Contrary to this approach, we argue that artificial intelligence, including in the field of criminal and penitentiary justice, should not be conceived as an autonomous

⁸ Ethan Mollick, *Co-inteligență, Cum să trăiești și să muncești cu AI*, Publica Publishing House, Bucharest, 2025, p. 67-68.

⁹ Yuval Noah Harari, *Nexus: A Brief History of Information Networks from the Stone Age to AI*, Penguin Random House, London, 2024, p. 200.

'extraterrestrial intelligence,' but rather as a tool created, trained, and limited through human will and legal norms. The risk of losing control does not derive from the existence of technology itself, but from the absence of adequate mechanisms of governance, transparency, and democratic oversight concerning its use.

In this regard, intelligent control may be defined as a model of supervision that uses available data to support human decision-making, without substituting it. Unlike absolute prohibition, intelligent control does not seek the complete elimination of potentially problematic behavior, but rather its management within a regulated and predictable framework.

Applied to the execution of sentences, these requirements imply that any digital mechanism intended for the monitoring or filtering of communications must operate within a predictable, verifiable, and controllable legal framework. Persons deprived of liberty must benefit from sufficient safeguards enabling them to understand the existence and nature of the restrictions imposed, as well as from the effective possibility of challenging measures considered excessive or unjustified. In the absence of such guarantees, digital control risks acquiring an opaque character that is difficult to subject to genuine judicial review.

Similarly, the requirements imposed by the European Union General Data Protection Regulation (GDPR) become essential within a system based on digital monitoring and technological traceability. The collection, storage, and use of data generated through digital communications must comply with the principles of legality, proportionality, purpose limitation, and data minimization. The existence of a custodial enforcement regime cannot justify the establishment of unlimited surveillance mechanisms or the

undifferentiated use of the personal data of convicted persons.

At the same time, one of the central elements of the legitimacy of such a model concerns the prohibition of the autonomous automation of restrictions on rights. The use of algorithmic instruments for identifying risks, filtering communications, or signaling behaviors considered problematic cannot lead to the elimination of meaningful human intervention from the decision-making process. In a state governed by the rule of law, restrictions upon the exercise of fundamental rights must remain the result of an individualized human assessment carried out in relation to the concrete circumstances of each situation.

From this perspective, the principle of human oversight does not represent a mere procedural formality, but rather a structural safeguard against the transformation of technology into an autonomous authority of penitentiary control. Human intervention must be genuine, effective, and capable of correcting or invalidating the conclusions generated by the technological systems employed. Technology may support penitentiary administration in the management of risks and in the organization of control; however, it cannot substitute legal responsibility and human judgment.

At the same time, the legitimacy of intelligent control presupposes the existence of clear mechanisms of auditability and traceability. Any operation involving the monitoring, filtering, or restriction of communications must be capable of subsequent verification from the perspective of its legality and proportionality. Auditability thus becomes an essential condition for preventing arbitrariness and for maintaining effective judicial oversight over the manner in which technology is used in the execution of sentences.

In reality, the fundamental issue is not whether the penitentiary enforcement system

should employ digital instruments and intelligent control mechanisms, but rather the manner in which these may be integrated without affecting the fundamental structure of the legal safeguards specific to the rule of law. The digital transformation of society renders the adaptation of the execution of sentences to new technological realities inevitable; however, such adaptation cannot be achieved through the autonomous transfer of decision-making power to algorithmic systems.

7. Conclusions

The digital transformation of society profoundly modifies the conditions under which the social reintegration of persons deprived of liberty may be achieved. In a social environment in which communication, education, family relationships, and professional activities are increasingly mediated through technology, maintaining an enforcement model constructed almost exclusively upon the exclusion of digital communications becomes increasingly difficult to reconcile with the reintegrative purpose of the execution of sentences.

The present analysis has demonstrated that the fundamental issue does not lie in the existence of control over digital communications, but rather in its generalized, undifferentiated, and disproportionate character. Maintaining an almost absolute prohibition concerning the use of telecommunication devices risks

transforming detention not only into a deprivation of physical liberty, but also into a form of digital exclusion incompatible with contemporary social realities.

In this context, the transition toward a model of intelligent control appears to constitute a possible solution of balance between the requirements of penitentiary security, the protection of fundamental rights, and the necessity of adapting the enforcement system to the technological transformations of society. The use of mechanisms of differentiated monitoring, technological filtering, and digital traceability may allow the exercise of effective control without completely eliminating access to regulated forms of digital communication.

Nevertheless, the legitimacy of such a model depends fundamentally upon the existence of clear legal safeguards concerning transparency, proportionality, judicial oversight, and effective human intervention. Technology must not become a substitute for human decision-making, but rather a support instrument for penitentiary administration in the management of concrete risks and in the individualization of the execution of sentences.

Ultimately, the real challenge is not exclusively technological, but rather legal and institutional: namely, how to adapt the execution of sentences to the realities of a digitalized society without compromising the fundamental principles of the rule of law and the profoundly human dimension of criminal justice.

References

- La Justice Prédicative, Actes Du Colloque du 12 Février 2018 organisé par L'ordre Des Avocats au Conseil d'état et À La Cour De Cassation a l'occasion de son bicentenaire en partenariat avec L'Université Paris-Dauphine PSL, Paris, Dalloz, 2018.
- Burgelin, Jean Francois, Sur le rôle de l'expert, v. J. Sainte-Rose, « Le juge face à la science », in *Principes de justice. Mélanges en l'honneur de Jean Francois Burgelin*, Dalloz, Paris, 2008.
- Chiş, Ioan, Chiş, Alexandru Bogdan, *Executarea sancţiunilor penale*, Curs universitar, Ediția a II a revizuită și adăugită, Universul Juridic Publishing House, Bucharest, 2021.

- Garapon, Antoine, Lassègue, Jean, Justice Digitale: Révolution Graphique et Rupture Anthropologique, Presses Universitaires de France (PUF), Paris, 2018.
- Harari, Yuval Noah, Nexus: A Brief History of Information Networks from the Stone Age to AI, Penguin Random House, London, 2024.
- Marshall, Tony F., Restorative Justice: An Overview, Kindle Edition, Coventry Lord Mayor's Committee for Peace & Reconciliation, Coventry City Council, United Kingdom, 2018.
- Mollick, Ethan, Co-inteligență, Cum să trăiești și să muncești cu AI, Publica Publishing House, Bucharest, 2025.
- Toon, Nigel, How AI Thinks: How We Built It, How It Can Help Us, and How We Can Control It, Transworld Publishers, Penguin Random House, London, 2024.