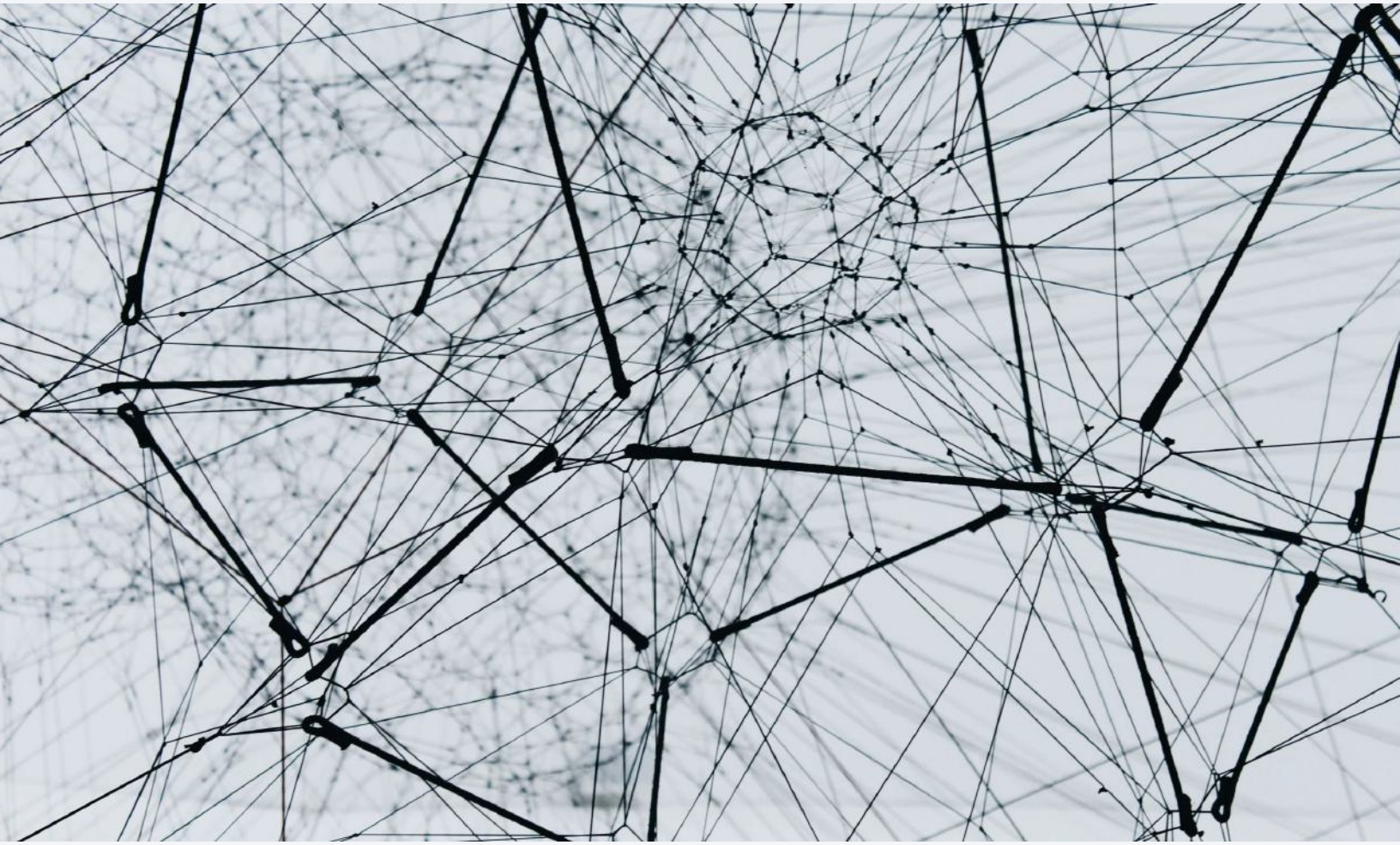


DIGITAL TRANSFORMATION IN PRISONS:

CONSIDERATIONS FOR INTEGRATING ICT AS THE BACKBONE OF ALL ASPECTS OF PRISON OPERATIONS

PRODUCED BY:

THE EUROPRIS ICT EXPERT GROUP

OCTOBER 2025

Co-funded by the European Union

ABOUT EUROPRIS

The European Organisation of Prison and Correctional Services (EuroPris) is a membership association founded in 2011. The initiative to establish EuroPris was taken during the Swedish EU Presidency in 2009 and was brought forward by the European countries of the International Roundtable for Correctional Excellence.

Membership is open to those European national Prison and Correctional Administrations who are able and willing to support the agreed aims and objectives of EuroPris. Public institutions or organisations in the Council of Europe region, which provide prison or correctional services on a legal or statutory basis can become members of EuroPris.

EuroPris brings together practitioners in the prisons' arena with the specific intention of promoting ethical and rights-based imprisonment, exchanging information and providing expert assistance to support this agenda. The organisation exists to improve cooperation among European Prison and Correctional Services, to improve the lives of prisoners and their families, enhancing public safety and security; reducing re-offending; and advancing professionalism in the prisons' field.

EuroPris
Bezuidenhoutseweg 20
2594 AV, The Hague
Netherlands
www.europris.org
secretariat@europris.org

The opinions expressed in this paper have been prepared in good faith and do not necessarily represent the views of the European Commission.

TABLE OF CONTENT

1. INTRODUCTION 2
1.1 Digital Transformation in Prisons 2
1.2 Key Areas of ICT Application in Prisons 2
2. STRATEGY, CONCEPT, AND CULTURE 4
3. BUDGET AND CHANGE MANAGEMENT 6
4. INFRASTRUCTURE AND TECHNICAL QUESTIONS 7
5. DESIGN OF DIGITAL SERVICES 8
5.1 Risks and Needs of Providing Digital Services 8
5.2 Prison Security 9
5.3 Digital Rehabilitation 10
5.4 Digital Skills 10
5.5 Collaboration with Stakeholders 11
5.6 The Impact and Risks of Public Procurement 12
6. RESEARCH AND FEEDBACK 13
6.1 Feedback and Research to Support Prison Design 13
6.2 Feedback and Research to Support Rehabilitation 14
6.3 Feedback and Research to Support Security and Decision Making 14
7. USE OF ARTIFICIAL INTELLIGENCE - FUTURE OF PRISONS 15
7.1 Artificial Intelligence in Design, Construction, and Maintenance of Prisons 15
7.2 Artificial Intelligence in Security, Safety of Prisons and Staff Practices 16
7.3 Artificial Intelligence and Services for Prisoners and Prison Administration 16
8. CONCLUSIONS 17
9. LITERATURE (FOR FURTHER READING) 18

Click on the page number to navigate to chapters.

EXECUTIVE SUMMARY

This paper, produced by the EuroPris ICT Expert Group, explores how information and communication technology (ICT) is transforming European prison systems. ICT is not simply a technical upgrade - it represents a strategic and cultural shift that impacts security, administration, rehabilitation, and reintegration. The concept of the "smart prison" envisions digitally connected environments where surveillance, communication, and offender management tools enhance safety while also supporting education, healthcare, and family contact. Importantly, technology should complement, not replace, human interaction, which remains essential to rehabilitation.

The implementation of ICT requires defined strategies, adequate budgeting, and change management, as well as addressing challenges such as procurement regulations, vendor lock-in, and the integration of new technologies into both old and newly constructed facilities. Infrastructure must be robust, with secure and redundant systems in place to protect sensitive data and ensure uninterrupted operations.

Digital services must be designed with different prisoner groups in mind, considering both opportunities and risks such as cybercrime, vandalism, and misuse. Training is crucial for both staff and prisoners, as digital literacy is increasingly a basic skill for reintegration into society. Collaboration with external stakeholders, including NGOs and educational or health providers, is also essential to deliver services effectively and securely.

The report serves EuroPris members and underlines the importance of research and continuous feedback in evaluating the effectiveness of digital tools, ensuring they genuinely support security, rehabilitation, and organisational efficiency. It also addresses the emerging role of artificial intelligence (AI), which can be used in the design and maintenance of prison buildings, in security systems such as monitoring and access control, and in services for prisoners like rehabilitation programs, education, and resource management. However, AI should always remain a tool that assists staff rather than replaces them, in line with ethical guidelines and human rights principles.

In conclusion, ICT in prisons is framed as a means to support staff, enhance security, and facilitate rehabilitation and reintegration. Technology is not an end in itself but a tool that, if implemented ethically and strategically, strengthens the human-centred mission of correctional services in Europe while aligning with modern expectations of efficiency, transparency, and respect for fundamental rights.

ACKNOWLEDGEMENTS

This paper is published by EuroPris – the European Organisation of Prison and Correctional Services. It was written by EuroPris' Information Communication and Technology in Prisons Expert Group: Marjan Lukavečki (Specialist in the Head Office for the Prison System and Information Security Adviser at the Ministry of Justice and Public Administration, Croatia), Marloes van de Braak (Project Manager of ICT Projects at the Dutch Custodial Institutions Agency), Hubert Unger (Senior ICT Manager within the Austrian Ministry of Justice), Berker Küçükçetin (Chief Officer responsible for ICT projects at the GDPDH, Turkey), Jacques Hensen (ICT Manager at the Administration Pénitentiaire, Luxembourg), Maria Puerto Solar (Prison Officer Programme Coordinator, Spain), Antonio Pastor Peral (ICT Projects Coordinator of the Catalonian Prison Service), and Donna Creaven (Director of ICT and Corporate Services with the Irish Prison Service). This Expert Group is also coordinated by EuroPris' Deputy Director, Justina Dzienko.

1. INTRODUCTION

This paper, developed from insights provided by members of the EuroPris ICT Expert Group, explores the increasingly critical role of Information and Communication Technology (ICT) in prison systems. As technology continues to evolve rapidly, it significantly impacts various facets of prison management. ICT is reshaping the entire prison environment—including security systems, communication, offender management, administrative processes, education, rehabilitation, and data analytics. The paper outlines key areas of ICT application and presents a structured approach to integration, distinguishing three essential levels: technical, procedural, and legislative.

While the paper focuses on ICT as a foundational tool in modern prison systems, it also emphasises the need to carefully consider how Artificial Intelligence (AI) can be introduced to support and enhance prison operations without compromising security. AI represents a fundamentally different paradigm, with the potential to revolutionise many aspects of prison management and operations, while also introducing new layers of complexity to ICT governance within European prison environments.

1.1 DIGITAL TRANSFORMATION IN PRISONS

The integration of ICT in prisons is not merely a technological enhancement—it offers a transformative opportunity to rethink how prison systems function and interact with the broader criminal justice framework. This transformation demands close collaboration between prison professionals and ICT specialists to design, evaluate, and manage technologies and infrastructure such as networks, servers, and equipment rooms.

It is important to recognise that whole Europe, including European Union (EU) member states, are at varying stages of ICT adoption within their prison systems. The level of integration and technological sophistication differs widely across countries due to variations in policy approaches, financial resources, technological priorities, and strategic focus. These disparities reflect broader socio-economic differences across Europe. By sharing insights and experiences, countries at different stages of ICT implementation can learn from one another. This collaborative exchange allows those with advanced systems to share best practices and lessons learned, while those in earlier phases can benefit from guidance and support.

A clear distinction must be made between implementing ICT in older prison buildings and integrating it into the design of newly constructed facilities. New buildings can be purpose-built to accommodate the cabling and equipment required for modern ICT systems. In contrast, retrofitting older facilities presents significant challenges due to structural and architectural constraints that limit cable routing, workstation placement, and the location of equipment rooms. Additionally, heritage or historically significant buildings may pose aesthetic and practical objections to surface-mounted ICT installations. Therefore, ICT integration in older prisons must be carefully tailored to the unique characteristics and limitations of each facility.

1.2 KEY AREAS OF ICT APPLICATION IN PRISONS

The scope of ICT interventions in prison systems is extensive, ranging from basic communication tools to advanced surveillance technologies, data management platforms, and AI-driven applications. To ensure effective implementation, ICT must be approached with a clear and structured plan, organised across three levels: technical, procedural, and legislative. For clarity and ease of analysis, the following key areas of ICT application are identified:

1. **Security Systems**: Prisons increasingly rely on ICT-based solutions for a wide range of security functions. These include advanced video surveillance, access control systems, perimeter monitoring (including drone detection), and integrated alarm systems. Such technologies are essential for monitoring activities, detecting intrusions, and ensuring the safety of both staff and inmates.

2. **Communication Systems**: ICT plays a vital role in facilitating communication within prisons. It enables monitored and controlled telephonic and messaging services (audio and video) for prisoners to maintain external contact, while also supporting internal communication among staff.

3. **Offender Management**: ICT systems are crucial for managing offender records, tracking movements, and monitoring behaviour. Centralised databases containing comprehensive prisoner information are key to effective prison administration.

4. **Administrative Systems**: ICT streamlines administrative functions such as inventory management, procurement, human resources, and financial operations. These systems improve efficiency and reduce manual workloads.

5. **Rehabilitation, Health, Training, and Education**: ICT enables access to health services, educational programs, vocational training, and psychosocial support. These initiatives are vital for skill development, personal growth, and reducing recidivism among released prisoners.

6. **Data Analytics and Reporting**: ICT allows for the analysis of large volumes of prison-generated data. Insights derived from this data help identify trends, anticipate security risks, and inform policy and management decisions.

To support effective ICT planning and implementation, it is essential to consider the following three levels:

1. **Technical Level**: This encompasses the hardware and software components of ICT systems. It includes infrastructure deployment, such as servers, networks, and data management systems, as well as the selection and implementation of technologies like surveillance cameras and management software. Maintenance and system upgrades are also part of this level.

2. **Work Procedures Level**: This focuses on integrating ICT into daily prison operations. It involves staff training, adapting workflows to incorporate ICT solutions, and developing new procedures for tasks such as data entry, prisoner tracking, and communication protocols. The aim is to enhance operational efficiency and security without disrupting essential services.

3. **Legislative Level**: This ensures that ICT implementations comply with relevant laws and regulations, including privacy and data protection laws, and legal frameworks governing surveillance and communication. It also involves creating policies to regulate ICT use, such as guidelines for data access, AI deployment, and communication monitoring.

2. STRATEGY, CONCEPT, AND CULTURE

The concept of the "smart prison" has emerged as a progressive step in the evolution of ICT applications within correctional facilities. By integrating advanced technologies, such as **Internet of Things (IoT)** sensors[1], AI-powered surveillance systems, and biometric solutions, smart prisons have the potential to fundamentally transform traditional incarceration models. Envisioning prisons as digitally connected ecosystems enables enhanced security while supporting rehabilitation and reintegration.

The term "smart" carries different meanings depending on the jurisdiction and prison system. Its interpretation varies across countries and regions. In some contexts, "smart" refers to more efficient ways of working and creating barrier-free, user-friendly experiences. For example:

- **Service Delivery for People in Custody**: This includes access to health and wellbeing services, education, language support, and prison operations such as biometric movement tracking, self-service kiosks, visitation scheduling, and translation tools via in-cell devices.

- **Digital Service Delivery for Staff and Partners**: Smart devices enable staff and other stakeholders to work more safely and accurately, supporting tasks such as accessing prisoner information, managing sentences, maintaining facilities, and overseeing inventory. These tools also free up time for more meaningful responsibilities.

Smart prison technologies also play a vital role in preparing prisoners for life in a digitally driven society, contributing to successful resocialisation. They allow prisoners to maintain family connections through in-cell communication and video conferencing. For instance, Finland's Smart Prison model treats the prison as a learning environment for a crime-free life, where digital services are integrated into daily routines to support rehabilitation and reintegration. This approach requires prison staff to adopt new working methods, including guiding prisoners in selecting appropriate digital services.

Governments and public services are increasingly embracing the "smart" concept to modernise operations and drive strategic shifts that support citizens, economic growth, and sustainable development. A smart public service understands the needs and preferences of its citizens and delivers seamless digital experiences across all aspects of life.

Smart technologies include devices, systems, and environments that interact intelligently with users and other technologies. They encompass intelligent products, AI, and self-service computing principles applied to systems and infrastructure. Importantly, "smart" is not just about adopting new technologies; it represents an organisational transformation in processes, priorities, and culture.

The rise of digital technologies presents an unprecedented opportunity to revolutionise correctional facility management. By implementing comprehensive digital solutions—including network and security infrastructure, Wi-Fi access for staff, and digital tools for inmates and administrative processes- prisons can streamline operations and foster safer, more secure, and efficient environments.

[1] Internet of Things (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communication networks. The IoT encompasses electronics, communication, and computer science engineering. "Internet of things" has been considered a misnomer because devices do not need to be connected to the public internet; they only need to be connected to a network and be individually addressable.
See: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

European prison services should consider identifying strategic business needs that support digital development and transformation. A digital strategy serves as a roadmap for continuous quality improvement across all areas, including prisoner journeys, staff experience, new operational processes, digital platforms, and governance. Modernising services through digital development is essential to deliver transparent, tailored, and innovative solutions that improve efficiency and effectiveness for both prisoners and staff. However, it is crucial to ensure that ICT does not replace meaningful human interaction and face-to-face rehabilitative services, which must remain a priority. Striking a balance between technological integration and a human-centred approach is vital. This principle is also central to the Council of Europe's recommendations on the ethical use of AI and digital technologies in prison and probation services, which will be discussed later in this paper.

As correctional systems navigate this evolving digital landscape, there is a growing need for practical guidance on how to apply principles within smart prison models. The next section aims to support prison services in developing smart environments solutions in a balanced and sustainable way that are secure, human-centred, and operationally effective.

SMART PRISON CONCEPT: KEY CONSIDERATIONS AND RECOMMENDATIONS

Staff Digital Tools

Prison services are encouraged to enhance user experience by automating low-value manual tasks and improving overall system performance. It is recommended to implement a targeted organisational dashboard to support internal performance monitoring. Staff autonomy should be increased in managing rosters, schedules, and leave. Additionally, opportunities for online learning and professional development should be expanded.

Digital Prisoner Services

Prison services are encouraged to develop a digital operating model that improves the prisoner journey, balances digital innovation with human interaction, and boosts productivity across the prison estate. It is also recommended to fully leverage digital tools for the benefit of both prisoners and staff, while addressing digital literacy gaps.

Digital / Smart Prison Concept

Prison services are encouraged to define the concept before selecting ICT solutions to ensure ethical, balanced, and rehabilitative use of technology. They should promote digital rehabilitation focused on work, education, and training. It is also recommended to facilitate formal and informal communication with courts and prisoners' families. Prison infrastructure should be advanced to allow prisoner movement without constant supervision. Additionally, electronic access to services such as ordering from the tuck shop, scheduling visits, and attending medical appointments should be enabled.

New Prison Culture

Modern prisoners, especially younger ones, are increasingly familiar with technology in daily life. Also, public expectations are rising for prison services to be technologically fluent and modernised. Governments also expect prison systems to operate advanced digital platforms and integrate with other justice sector branches. Social demands include maintaining family connections through video calls, helping children with homework, and improving spousal communication. Digital labour opportunities are emerging: in Finland, prisoners can work remotely from open prisons if they own a business or perform data annotation tasks using secure laptops in closed prisons, while the Netherlands is exploring mobile phone and Wi-Fi access for external job opportunities. Long-term prisoners require basic digital skills training to use digital services during incarceration and after release. Finally, access to digital services within prison is increasingly viewed as a human or fundamental right, as real-time access to education, healthcare, and other services depends on digital connectivity.

Joint Development and User-Centred Design

A key consideration is to begin with the prisoner by identifying the target segment or profile to guide design decisions. In new prison facilities, ICT planning should be involved from the earliest stages. Caution is advised with specifications: due to rapid technological change, finalising tech orders late in the project can help avoid obsolescence. Hardware and cabling design should be prioritised to allow easy upgrades. Close collaboration with stakeholders in care, rehabilitation, and security is recommended to align expectations with realistic outcomes. Finally, it is important to clearly define which systems are intended for implementation.

3. BUDGET AND CHANGE MANAGEMENT

Budget planning is a critical component when evaluating the value of digital initiatives against the overall cost of prison operations. This assessment must account for initial investment costs, potential disruptions to daily operations, and the broader impact on prison functions. Key considerations include the risk of vendor lock-in, which can limit future flexibility and drive-up long-term costs, as well as ongoing expenses such as system maintenance and annual licensing fees.

Equally important is the issue of interoperability. Technologies must be capable of integrating seamlessly with existing systems to ensure scalability, adaptability, and long-term sustainability. Interoperable solutions help mitigate financial risks and support the development of a resilient digital infrastructure.

Introducing ICT into prison systems can be particularly challenging due to rigid and formal procurement procedures. These processes are often governed by strict guidelines and requirements, which can hinder the swift adoption of innovative solutions. Therefore, procurement must be approached strategically to ensure that selected technologies meet operational needs, deliver long-term value, and remain compatible with existing systems, all within regulatory and budgetary constraints, as highlighted in the Introduction.

BUDGET MANAGEMENT CONSIDERATIONS

- **Organisational Fit**: Assess the organisation's specific needs, goals, and expectations.
- **Cost-Benefit Analysis**: Evaluate whether the anticipated benefits justify the investment.
- **Types of Costs**: Consider purchasing and installation expenses, potential downtime, and disruptions to prison operations.
- **Usability**: Determine whether the system is intuitive and accessible for prisoners. Can it be used effectively without extensive training?
- **Procurement Strategy**: Select systems that align with procurement regulations while meeting operational requirements.
- **Licensing**: Account for recurring licensing fees and long-term financial commitments.
- **System Access**: Clarify whether the system uses open or closed protocols and whether external service providers can access it.

OPERATIONAL AND CHANGE MANAGEMENT

- **Training Requirements**: Plan for training staff and/or prisoners to use the system effectively.
- **Resource Intensity**: Assess whether the system demands significant staff involvement or leads to inefficient resource use.
- **Benefit Evaluation**: Identify both operational advantages and cost-efficiency outcomes.
- **Organisational Planning**: Address staff management, resource allocation, and stakeholder collaboration during implementation.

APPLICABILITY AND INTEGRATION ACROSS FACILITIES

Assess whether the digital concept can be adapted to different types of facilities—particularly older versus newly constructed units. Consider the integration of existing systems and technologies, such as:

- CCTV surveillance
- Cell call systems
- In-cell television systems
- Electronic locking mechanisms
- Fire alarms and life safety systems
- Building management systems

A key question is whether these legacy systems can communicate effectively with new digital platforms without encountering licensing or copyright barriers. Ensuring compatibility is essential for cohesive and cost-effective digital transformation across the prison estate.

4. INFRASTRUCTURE AND TECHNICAL QUESTIONS

Prisons depend on a wide range of critical infrastructure to support daily operations. To minimise disruptions caused by power outages, it is essential for prisons to implement redundant power systems, such as backup generators and uninterruptible power supply (UPS) units. When functioning effectively, these systems significantly reduce downtime and prevent the need for extensive recovery procedures across the site.

The integration of digital devices, such as laptops, tablets, and smartphones, into prison environments offers both opportunities and challenges. These tools can support education, vocational training, and prisoner communication. However, their use must be tightly regulated to prevent security breaches and illicit activity. Establishing secure Wi-Fi networks or providing restricted internet access in supervised settings is vital to managing the risks associated with unauthorised online behaviour, though it introduces its own complexities.

To safeguard prison operations, low-current cabling must be configured to ensure that faults, equipment failures, or cyberattacks do not compromise security systems or expose sensitive data. This requires a segmented infrastructure tailored to specific functions and operational needs. It is important to distinguish between different infrastructure types during construction and maintain this separation throughout the facility's lifecycle when deploying new technologies or digital applications:

- **Voice, Data, and Image Infrastructure**: Used by prison administration staff and external partners for IT systems, telephony, videoconferencing, and related services.
- **Sensitive Infrastructure for Prisoners**: Includes television, telephones, and digital services in cells and communal areas.
- **Security Infrastructure for Facility Management**: Covers anti-intrusion systems, video surveillance, intercoms, access control, fire safety, and building management systems (BMS).

Ideally, security systems should not be outsourced beyond the prison they serve. Each network should be built with redundancy, meaning duplicate cores hosted in separate, secure technical rooms that can take over in case of failure. To support the deployment and expansion of low-current systems, prisons must be equipped with sufficient technical rooms designed for resilience, access control, and future scalability.

Common challenges include limited space for equipment installation and maintenance, as well as inadequate air conditioning. Another critical requirement is the physical separation of networks: cables must be routed through distinct and distant trays and ducts. These pathways should include reserves for future installations and inspection access. In many existing prisons, low-current cables are visibly exposed due to insufficient duct space or inaccessible ceiling structures, highlighting the need for better planning and infrastructure design.

While new buildings may allow for flexible technology choices (e.g., wired vs. wireless solutions), older facilities often lack such options due to architectural constraints. It is therefore essential to plan thoroughly to ensure that systems for staff and prisoners can coexist effectively. Maintenance and repair of facility equipment is crucial, and remote servicing offers a cost-effective and efficient solution. However, it introduces security risks that must be addressed. Remote diagnostic tools and troubleshooting techniques can resolve hardware issues without onsite visits, reducing downtime and operational disruption.

Strong security protocols are essential to protect sensitive data and prevent unauthorised access to critical systems. Correctional institutions employ robust measures such as encryption, access controls, and regular security audits to mitigate the risk of cyberattacks and data breaches. In addition, comprehensive surveillance systems—including CCTV, motion sensors, and biometric technologies- enable continuous monitoring of prisoner activity and allow for timely intervention when needed.

The integration of advanced infrastructure and rigorous security protocols is key to strengthening prison environments and reducing risk. As institutions explore AI-driven solutions, it is vital to approach implementation with care. By embracing innovation and adopting a proactive stance on security management, correctional facilities can uphold the highest standards of safety, efficiency, and operational integrity.

5. DESIGN OF DIGITAL SERVICES

5.1 RISKS AND NEEDS OF PROVIDING DIGITAL SERVICES

The integration of technology into prison design aims to enhance security, living conditions, rehabilitation, and reintegration through digital means. To achieve these goals effectively, prisoners must be profiled according to their specific needs and risks within individual units or services. This profiling is essential to ensure that ICT investments are targeted and responsive to rehabilitative needs.

Prisoners represent diverse segments, each with distinct digital requirements. These groups may include women, youth and minors, ethnic and religious minorities, gender and sexual minorities, elderly individuals, disadvantaged populations, members of organised crime networks, and short-term offenders.

While some needs overlap, each group also presents unique challenges. Digital solutions must be flexible and inclusive, offering “something for everyone.” This includes ensuring compatibility between online and offline (face-to-face) services, allowing prisoners to take responsibility for aspects of their rehabilitation while receiving staff-led support.

Except in specific cases involving high-risk profiles or specialised care, prison facilities should be designed to adapt to changing demands. For example, a unit currently housing low-risk prisoners may not require internet access or advanced security installations, but this could change over the next decade. Therefore, prison design must accommodate the deployment, evolution, and even reversal of digital technologies.

Digital services must also account for risk factors to avoid inadvertently enabling criminal, harmful, or threatening behaviour from within prison. Risks include cybercrime, online harassment, sexual offences, fraud, and planning serious crimes. These can be mitigated by assigning different user rights based on prisoner profiles. For instance, remand prisoners or those serving long sentences under confinement may have restricted communication rights. Systems should prevent misuse, such as one prisoner accessing another's credentials or personal data (e.g., bank accounts or IDs). Vandalism, whether intentional or due to a lack of digital skills, also poses a threat to devices and software. Given the rapid pace of technological change and the fragility of some systems, these risks must be factored into ICT-led prison design.

To prevent purely recreational use of digital systems, staff should guide prisoners in using the technology to support their rehabilitation. This includes helping them identify services that align with their personal development goals.

Architectural design must also protect digital tools and active security systems from degradation. For example, televisions should be vandal-resistant and mounted on secure, non-removable supports. In cells housing prisoners with violent tendencies, screens should be embedded into walls, shielded against impact, and free of exposed cables that could be used for self-harm. While such integration is common for televisions, it is not yet standard for digital tablets.

Regarding active security infrastructure, any space intended for future equipment or wiring must include features such as accessible false ceilings, cable trays, and sufficient ceiling height to accommodate future installations. Every area that may eventually host new technologies for prisoners, staff, or management should be designed with foresight to ensure physical protection and ease of installation.

5.2 PRISON SECURITY

Security installations in prisons typically include video surveillance, radio transceivers, staff telephony systems, access control mechanisms (e.g., remote or badge-based door opening), and various intercom systems—for detainees in cells, secure communication between guard posts, or door access requests.

Additional systems include perimeter detection, mobile phone jamming, anti-drone technologies, alarm systems, biometric identification, and, in some cases, sound systems. These technologies serve dual purposes: ensuring the safety of prisoners and staff, and preventing unauthorised contact with the outside world, such as drug trafficking or other illicit activities.

ICT solutions can also improve prisoners' quality of life by enabling access to phones, tablets, videoconferencing, and digital media libraries. Digital contact with family and friends—via video calls, emails, or messaging platforms—is highly valued by prisoners. However, these interactions raise technical and security concerns, particularly around verifying the identity of the external party. For example, Catalonian prisons use facial recognition for sign-in, while Finnish prisons may require ID verification at the start of a video call. The willingness of the external party to engage in such contact must also be considered.

Supporting digital communication with the outside world requires careful planning to address security risks. Additionally, friends and family members may lack the digital literacy needed to use these systems. Clear instructions should be provided—ideally via the prison's website. In Catalonia, a chatbot is being developed to guide users through the process. Raising awareness about available support services, such as digital assistance from device retailers or NGOs, is also important.

While AI and advanced systems can enhance surveillance and security, over-reliance on these technologies risks eroding staff expertise in monitoring and intervention. The final responsibility for prison security must remain with human personnel. Preserving and developing staff skills is essential as prisons modernise, ensuring that technological advancements complement rather than replace human oversight.

5.3 DIGITAL REHABILITATION

Digital rehabilitation refers to the use of technology to enhance rehabilitative efforts within prisons. It can elevate the quality of rehabilitation, expand the range of available services, increase access to external support, and add value to prison practices that traditional, non-digital environments may lack. For vulnerable populations, the anonymity and autonomy offered by digital services can be particularly beneficial.

To reduce recidivism, ICT solutions can be designed to support key areas of rehabilitation and reintegration. These include substance abuse treatment, behavioural therapy, psychosocial and mental health care, education, vocational training, and family support. Digital platforms can facilitate access to these services, whether through personal or shared devices used independently or in collaboration with prison staff or external providers. While some software includes built-in features for these areas, often the platform serves as a conduit, with content delivered by external organisations or the prison system itself, such as rehabilitative programs, self-help modules, or video consultations.

Various software solutions exist for internal prison management and prisoner communication, with some offering limited external connectivity. The choice of hardware (e.g., tablets, laptops) and operating systems (e.g., Windows, Linux), along with productivity tools like Office suites, must be carefully considered. Prisons typically define restrictions for external communication, such as internet access controls (whitelists/blacklists), video call permissions, and email usage. Selecting appropriate web-based services requires a clear understanding of prisoners' risks and needs, and should align with the goals of digitalisation, whether focused on rehabilitation, reintegration, human rights, cost-efficiency, or a combination of these.

Collaboration is essential. NGOs, public service providers (in health, education, and vocational training), and private companies may all contribute to digital service delivery. These services must be co-designed with prison authorities to ensure they meet prisoners' specific needs and mitigate potential risks.

Digital services should complement, not replace, face-to-face rehabilitation. Compatibility between online and offline methods ensures continuity, allowing prisoners to benefit from both staff-led and self-directed learning. While some face-to-face interactions may occur via video calls or shared platforms, effective rehabilitation typically combines both formats. Many prisoners face challenges such as low literacy, poor concentration, or cognitive impairments, which can hinder their ability to engage with digital programs. These individual needs must be considered. Over-reliance on self-directed digital rehabilitation may also erode staff expertise in delivering personal, interactive support. The final responsibility for rehabilitation must remain with prison staff.

5.4 DIGITAL SKILLS

Digital literacy among prisoners, and staff, varies widely. Systems should be designed to be barrier-free: intuitive, easy to use, and self-explanatory, enabling self-learning where possible. Nonetheless, basic training should be provided initially, with ongoing support as new features or staff are introduced. Staff should be trained to a level where they can also instruct prisoners. Systems must cater to all skill levels and offer opportunities for skill development.

Basic digital competencies, such as using the internet, email, and office software, should be part of prisoners' training. If prison staff cannot deliver this training, external educators or NGOs should be engaged. Digital skills are essential for reintegration into modern society, where everyday tasks and communication increasingly rely on technology. They are also critical for pursuing education or employment. Without these skills, prisoners' risk further marginalisation.

Digital literacy also enables remote work opportunities within prisons, allowing inmates to engage in digital labour alongside traditional work forms. While permitted in many countries, this practice remains underutilised.

Each system should have sufficient staff trained as local administrators to manage daily operations and respond to risks. At the national level, there should be technically proficient administrators who can support field staff and liaise with system providers. Introducing new digital tools alters staff workflows, especially if the prison administration aims to shift roles from purely security-focused to more socially supportive functions. These tools should streamline and enhance daily tasks. Staff must understand the purpose of each system and recognise that its benefits depend on active engagement. The greatest risk is not misuse, but underuse, where staff and prisoners fail to explore the full range of features beyond basic functions like video calls.

5.5 COLLABORATION WITH STAKEHOLDERS

Most digital services for prisoners are delivered by external providers. Software is typically supplied by vendors, while web-based services may include civil, legal, private sector, and NGO platforms. These partners often already collaborate with prison services, but digitalisation introduces new forms of engagement. For stakeholders with limited resources, digital delivery reduces the need for travel and enables broader reach through secure online channels. For prisoners, digital contact can offer a lower-threshold, more anonymous and controlled way to initiate communication with external parties.

Security and privacy must be carefully managed, both technically and procedurally, when facilitating remote contact.

Successful deployment of digital technology in prisons requires close coordination with real estate managers to ensure installations are secure, sustainable, and cost-effective. This collaboration is vital across all phases:

- **Experimentation**: Testing products under optimal conditions.
- **Study**: Integrating technical and safety requirements into planning.
- **Installation**: Adjusting layouts and completing necessary works.
- **Acceptance**: Verifying that installations have not damaged existing infrastructure.

This coordination is equally important during prison construction or renovation.

Appointing a designated design champion is essential when introducing new digital tools or security systems. This individual should represent the prison's needs and validate the final solution. Their involvement should span the entire process, from design and procurement to delivery, commissioning, and handover.

5.6 THE IMPACT AND RISKS OF PUBLIC PROCUREMENT

Public procurement plays a pivotal role in the execution of major public administration projects, particularly in the implementation of ICT technologies within prisons, an essential component of the modern "smart prison" concept. Public procurement refers to the process by which public authorities, **such as government departments or local authorities, purchase work, goods or services from companies**. This process is governed by European and national legislation, which imposes strict procedural requirements and offers limited flexibility.

There are several types of public tendering procedures, including:

- Open procedure
- Restricted procedure
- Competitive negotiated procedure
- Competitive dialogue
- Innovation partnership
- Design contest

The European Union promotes open competition through these procedures, ensuring fairness and transparency. However, because prison services must adhere to prescribed processes and deadlines, public procurement introduces a range of risks and critical factors that can significantly affect project implementation, quality, and timelines.

Procurement is guided by core principles such as transparency, equal treatment, proportionality, and mutual recognition. While these principles uphold fairness, the rigid structure of procurement compels prison services to engage in detailed scope planning and precise requirement definition—both essential for accurate budgeting. As a result, procurement directly influences project costs, technology selection, vendor choice, and delivery timelines, while also introducing several risks.

Key Risks in Public Procurement:

- **Human Resource Constraints**: One of the most significant risks is the lack of adequate human resources. Successful procurement planning and execution require the expertise of a multidisciplinary team, not just procurement specialists, to define scope, expectations, and technical requirements accurately.
- **Bureaucracy**: While clearly defined procedures protect stakeholder rights, they can also be misused. Stakeholders dissatisfied with outcomes may exploit procedural rights to delay or halt progress, impacting project timelines and delivery.
- **Technological Obsolescence**: Long procurement cycles carry the risk of acquiring outdated technology. It is essential to plan for solutions that will remain relevant and effective at the time of project completion.
- **Financial Risks**: Extended procurement timelines can lead to price increases for goods or services, potentially exceeding budget forecasts and jeopardising project feasibility.
- **Legal and Compliance Risks**: These include non-compliance with procurement regulations, corruption, and contractors failing to meet agreed terms.
- **Vendor Lock-In**: This occurs when a prison service becomes dependent on a single supplier, making it costly or impractical to switch providers. Characteristics of vendor lock-in include:
    - Limited flexibility
    - Poor interoperability
    - Higher costs
    - Weak negotiating position
    - Long-term contractual obligations

To mitigate these risks, robust risk management practices must be embedded throughout the procurement process. This includes early stakeholder engagement, clear requirement definition, flexible technology planning, and continuous oversight to ensure compliance, transparency, and long-term value.

6. RESEARCH AND FEEDBACK

Introducing research mechanisms and feedback loops is essential to evaluate the impact and added value of digital systems in prisons. These insights enable continuous improvement and ensure that digital solutions evolve alongside broader prison practices.

This is particularly true for ICT software, where initial versions often fall short of expectations and must be refined through collaboration between vendors and users. Meaningful digital transformation can only occur when digital systems are developed to match the quality and effectiveness of traditional face-to-face services aimed at reducing recidivism.

6.1 FEEDBACK AND RESEARCH TO SUPPORT PRISON DESIGN

Within prison administrations, research may focus on digital tools, active security systems, or architectural design. However, such studies are sometimes disconnected from operational realities and conducted too early in the process to influence practical decisions, especially those involving real estate considerations.

In contrast, experimentation is a vital part of developing ICT services and installing active security equipment. It helps determine whether a prison can technically accommodate a given solution, particularly when the installation must be integrated into the facility's infrastructure.

These trials are typically conducted in existing prisons, which offer the advantage of established buildings, operational systems, and access to both staff and prisoners. For training services, relevant partners are often already involved; for security installations, the challenges they aim to address are already present.

Prison architecture and construction methods frequently pose obstacles to deploying digital systems. These include limitations in space functionality, the need for technical ducts to house cables and equipment, and the capacity of networks to handle new ICT workflows. For example:

- Mobile phone jamming may be ineffective in buildings with thick walls and floors that block signals inconsistently.
- Installing in-cell telephones may be hindered by narrow ducts that cannot accommodate additional wiring.
- Videoconferencing in visitation areas may be unfeasible due to insufficient room size for screens and equipment.

Feedback is crucial for evaluating the outcomes of digital tool or security equipment installations and guiding their improvement—especially before scaling up. It allows assessment of:

- **Relevance**: Does the solution meet the expressed needs?
- **Consistency**: Are the resources aligned with the intended goals?
- **Efficiency**: Are the deployed means appropriate for the results achieved?
- **Sustainability**: Can the benefits be maintained over time?
- **Flexibility**: Can the system adapt to changes during implementation?

6.2 FEEDBACK AND RESEARCH TO SUPPORT REHABILITATION

Research into ICT solutions for rehabilitation should clarify their benefits, including improved efficiency (e.g., reduced recidivism, enhanced well-being), support for basic rights, cost-effectiveness, and long-term sustainability. Beyond prisoner outcomes, it should also assess whether these solutions benefit staff and the wider prison organisation.

Evidence-based evaluation is essential. Can we demonstrate that digitalisation in prisons delivers measurable improvements? How can these benefits be operationalised and tracked? At a minimum, qualitative feedback should be collected from prisoners, staff, and management. To ensure objectivity and reliability, it's important to consider whether internal research is sufficient or if external research partners should be engaged.

Based on this research and feedback, best practices and policies should be defined and shared across all levels of the organisation. Maintaining and evolving the concept of digital rehabilitation—and the ICT systems that support it—must be an ongoing process informed by these insights.

6.3 FEEDBACK AND RESEARCH TO SUPPORT REHABILITATION

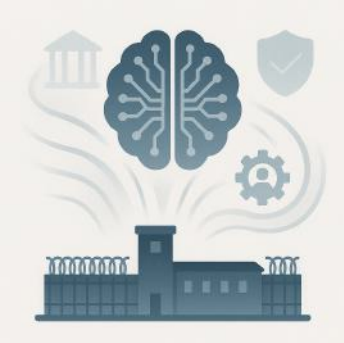
Security and decision-making are central to maintaining order, protecting the well-being of prisoners and staff, and preventing incidents such as escapes or disturbances. Continuous feedback and research are essential to strengthening these functions.

Feedback provides prison administrators with a dynamic tool to evaluate the effectiveness of current security protocols and identify areas for improvement. Input from prisoners can reveal vulnerabilities, abusive practices, or gaps in rehabilitation efforts. Staff feedback helps assess training adequacy, resource needs, and safety concerns.

Establishing formal feedback channels—such as suggestion boxes or anonymous reporting systems—empowers both prisoners and staff to share concerns without fear of reprisal. This fosters transparency, accountability, and ultimately enhances security.

Research supports evidence-based policy development and strategic decision-making. Academic studies, data analysis, and empirical research offer insights into emerging threats, successful practices in other facilities, and opportunities for innovation. Through research, prisons can adopt best practices, implement advanced technologies, and refine existing protocols.

In summary, feedback and research are foundational to improving security and decision-making in correctional settings. A continuous feedback loop identifies weaknesses, while research provides the evidence needed for informed decisions. Together, they contribute to a more effective, secure, and humane prison system.



7. USE OF ARTIFICIAL INTELLIGENCE - FUTURE OF PRISONS

The use of Artificial Intelligence (AI) in correctional settings should be guided by the Council of Europe's Recommendation CM/Rec(2024)5 regarding the Ethical and Organisational Aspects of the Use of Artificial Intelligence and related Digital Technologies by Prison and Probation Services. These principles define the purpose and boundaries of AI use, emphasising a human-centred approach. AI and related technologies should be applied legitimately and proportionately, and only when they:

1. Contribute to the rehabilitation and reintegration of offenders
2. Assist—rather than replace—prison and probation staff in their daily work
3. Support the criminal justice system, the execution of penal sanctions, and the reduction of recidivism

7.1 ARTIFICIAL INTELLIGENCE IN DESIGN, CONSTRUCTION AND MAINTENANCE OF PRISONS

AI offers significant potential to improve the efficiency and outcomes of prison design and construction. Through tools such as Building Information Modelling (BIM), AI can support simulations across various domains—functionality, structural integrity, thermal performance, natural lighting, acoustics, and more.

During real estate development, AI can be used to analyse specific spaces like cells and guard posts by integrating architectural, technical, ergonomic, and security-related data. This modelling could lead to standardised designs for these areas, verified through prototype testing, allowing architects to focus on more creative aspects of prison design.

During real estate development, AI can be used to analyse specific spaces like cells and guard posts by integrating architectural, technical, ergonomic, and security-related data. This modelling could lead to standardised designs for these areas, verified through prototype testing, allowing architects to focus on more creative aspects of prison design.

In large-scale construction or renovation projects, delays, design errors, and delivery mismatches can have serious financial and operational consequences. AI can help mitigate these risks by improving planning accuracy, enhancing site safety, and reducing environmental impact.

AI-enabled maintenance systems, when integrated with building management platforms, can optimise operations, forecast regulatory compliance, plan renewals, and support budget programming. However, full adoption of BIM from design through to maintenance remains limited, with gaps in data on detainee behaviour, prison work practices, and infrastructure ageing still to be addressed.

7.2 ARTIFICIAL INTELLIGENCE AND SECURITY-SAFETY OF PRISONS AND STAFF PRACTICES

AI is currently underutilised in prison security, except in a few countries, largely due to concerns around fundamental rights. Legal and regulatory safeguards must be in place before deploying AI in this domain. Nonetheless, the potential applications are clear. AI can support:

- Monitoring of detainees to detect violence, escape attempts, contraband trafficking, and unauthorised mobile phone use
- Access control systems to manage prisoner movement, simplify staff tasks, and organise visitations
- Communication monitoring, including phone restrictions and surveillance of external contacts

These technologies are evolving rapidly and must be considered in prison design and renovation. AI-driven systems may require:

- Larger technical ducts
- Expanded technical rooms
- Increased ceiling heights
- Structural adaptations (e.g., slab reservations, waterproofing modifications) to accommodate future installations

Prison administrations can initiate research and pilot projects to explore AI's role in supporting staff tasks—such as initial CCTV review, remote door control, and prisoner movement management. Technologies like drones, body cameras, and smart surveillance systems can assist in data collection and categorisation, but final decisions must remain with human personnel to preserve traditional management and human contact.

Biometric technologies, which often involve sensitive personal data, must comply with national laws and regulations. Jurisdictions may impose restrictions, underscoring the importance of legal compliance in AI deployment.

7.3 ARTIFICIAL INTELLIGENCE AND SERVICES FOR PRISONERS AND PRISON ADMINISTRATION

AI is increasingly used in offender management, human resources, rehabilitation, education, and training, though these applications are not directly tied to prison architecture.

In offender management, AI can assist to analyse prisoner data to assess risks and needs, recommend suitable unit placements, and suggest relevant services or programmes. These recommendations should support, not replace, human decision-making. Text analytics can also be used to extract insights related to support security and rehabilitation needs.

AI can enhance cost-effective and sustainable prison management by optimising resource use, including staff allocation, materials, and energy. Many European prisons face staffing shortages and operational challenges, and AI can help reallocate resources more optimally.

In rehabilitation, AI-powered solutions are already in use. Virtual reality (VR) and augmented reality (AR) are increasingly applied to support mental health, behavioural change, and skill development. Educational and vocational programmes also benefit from AI-enhanced tools. In Finland, prisoners participate in AI training through data annotation tasks. As technology evolves, AI is expected to play an even more transformative role in correctional services.

8. CONCLUSIONS

The integration of Information and Communication Technology (ICT) within prisons is no longer a question of if, but how. Across Europe, correctional services are at different stages of digital maturity, yet they all face the same imperative: to harness technology in ways that enhance security, support rehabilitation, and respect human rights. ICT must be recognised not as a goal in itself, but as a powerful enabler of modern, efficient, and humane prison systems and the backbone of all aspects of prison operations.

Several overarching lessons emerge from this guide. First, successful deployment of ICT requires a balance between technical infrastructure, organisational culture, and legislative frameworks. Without alignment across these three dimensions, even the most sophisticated technologies may fail to deliver their intended benefits and fall short of delivering meaningful impact. Second, digitalisation must be driven by clear strategic objectives, such as improving safety, operational efficiency, and facilitating rehabilitation, rather than by technological novelty alone.

The development of "smart prisons" presents both promise and complexity and offers both opportunities and challenges. Digital services can expand access to education, healthcare, family contact, and rehabilitative programmes, but they must complement, not replace, human interaction. Technology should empower staff, not diminish their professional expertise or reduce personal engagement with prisoners. Safeguards must be in place to address emerging risks, including cybercrime, overreliance on automated decision-making, and threats to privacy.

The growing role of Artificial Intelligence further underscores the need for ethical, transparent, and human-centred approaches. AI has the potential to optimise prison design, security, and resource management, while offering innovative tools for rehabilitation and educational. However, its use must remain proportionate, subject to democratic oversight, and consistent with European legal and human rights standards.

For EuroPris members, collaboration and knowledge-sharing will be key. No single administration can navigate the complex challenges of digital transformation alone. By learning from one another's experiences, whether in procurement, infrastructure design, staff training, or prisoner services, countries can avoid costly mistakes, accelerate progress, and develop interoperable, future-proof systems.

Ultimately, digital transformation in prisons is about preparing European correctional systems for the realities of the 21st century. It demands sustained investment, thoughtful change management, and above all, a commitment to using technology to build safer, fairer, and more rehabilitative environments. For directors, managers, and frontline staff, ICT provides a pathway not only to operational efficiency but to a prison culture that is more responsive, transparent, and reintegration-focused.

This paper is the result of the collective expertise and dedication of the EuroPris ICT Expert Group. Their work reflects a shared vision for the future of corrections, one where digital transformation is not a one-off initiative, but an ongoing journey. By approaching this journey strategically, ethically, and collaboratively, European prison services can ensure that ICT becomes the backbone of all aspects of prison operations, serving staff, prisoners, and society with integrity and purpose.

9. LITERATURE (FOR FURTHER READING)

Imandeka, E., Hidayanto, A., & Mahmud, M. (2024). Smart prison technology and challenges: a systematic literature review. International Journal of Artificial Intelligence (IJ-AI), 13(2), 1214-1226.

Jewkes, Y., & Reisdorf, B. C. (2016). A brave new world: The problems and opportunities presented by new media technologies in prisons. Criminology & Criminal Justice, 16(5), 534–551.

Järveläinen, E., & Rantanen, T. (2020). Incarcerated people's challenges for digital inclusion in Finnish prisons. Nordic Journal of Criminology. DOI: https://doi.org/10.1080/2578983X.2020.1819092

Kaun, A., & Stierenstedt, F. (2020). Doing time, the smart way? Temporalities of the smart prison. New media & society, 22(9), 1580–1599.

Knight, V. (2017). Digitizing the Prison: The Light and Dark Future. Prison Service Journal, 231, 22-30.
Knight, V., & Van De Steene, S. (2017). The Capacity and Capability of Digital Innovation in Prisons: Towards Smart Prisons. Advancing Corrections, Edition 3.

Lindström, B., & Puolakka, P. (2020). Smart Prison: the preliminary development process of digital self-services in Finnish prisons. https://icpa.org/smart-prison-the-preliminary-development-process-of-digital-self-services-in-finnish-prisons/

McDougall, C., Pearson, Torgerson, D. J., & Garcia-Reyes, M. (2017). The effect of digital technology on prisoner behavior and reoffending: a natural stepped-wedge design. Journal of Experimental Criminology, 13, 455–482.
Palmer, E. J., Hatcher, R. M., & Tonkin, M. J. (2020). Evaluation of digital technology in prisons. Ministry of Justice Analytical Series, UK.

Puolakka, P., & Van De Steene, S. (2021). Artificial Intelligence in Prisons in 2030. An exploration on the future of Artificial Intelligence in Prisons. Advancing Corrections Journal, 11, ICPA.

Puolakka, P. (2022). Implementing a Smart Prison in Finland. Advancing Corrections Journal, 14. ICPA.

Puolakka, P. (2024). Women Benefit More From Digital Rehabilitation Than Men. Advancing Corrections, 18, 145-158.

Puolakka, P., & Suomela, M. (2023). Digitalization Supports Human Rights in Finnish Prisons, Advancing Corrections Journal, 16, p. 50-61. ICPA.

Rantanen, T., Järveläinen, E., & Leppälahti, T. (2021): Prisoners as Users of Digital Health Care and Social Welfare Services: A Finnish Attitude Survey. International Journal of Environmental Research and Public Health, 18(11), 5528.

Rodrigues, A., & Fidalgo, S. (2024). The role of Artificial Intelligence (AI) in rehabilitation and in the reduction of the use of imprisonment. UNIO - EU Law Journal, 10(1), 42-53.

Smith, P. S. (2012). Imprisonment and internet-access: Human rights, the principle of normalization and the question of prisoners' access to digital communications technology. Nordic Journal of Human Rights, 30(4), 454-482.

Tilt, S. (2024). Exploring Prisoners' Use of Personal Computers. A thesis submitted in partial fulfilment of the requirements of Nottingham Trent University for the degree of Doctor of Psychology (DPsych) in Forensic Psychology.

Van De Steene, S., & Knight, V. (2017). Digital transformation for prisons: Developing a needs-based strategy. Probation Journal, 64(3), 256–268.

Yamamoto, M., Knight, V., Ross, S, & Burnett-Stuart, M., & Roberti, A. (2024). Digital Rehabilitation in Prisons. United Interregional Crime and Justice Research Institute (UNICRI).

EuroPris
Bezuidenhoutseweg 20
2594 AV, The Hague
Netherlands
secretariat@europris.org

Co-funded by the European Union