REPORT

On digital resources in detention

Julia Krikorian
Stéphanie Coye
European Prison Litigation Network

April 2019

EUROPEAN
PRISON
LITIGATION
NETWORK

This report is part of the research project EUPRETRIALRIGHTS from the consortium of partners :

Centre National de la Recherche Scientifique
Laboratoire SAGE, Université de Strasbourg
CESDIP, Université de Saint Quentin en Yvelines/Ministère de la Justice
European Prison Litigation Network
University of Utrecht, Montaigne Centre for Rule of Law and Administration of Justice
Helsinki Foundation for Human Rights, Poland
Dortmund University of Applied Sciences and Arts
University of Florence, L'Altro diritto - Inter-university Centre
Bulgarian Helsinki Committee
Ghent University, Institute for International Research on Criminal Policy
General Council of Spanish Bars
Pontifical University of Comillas

INTRODUCTION

The digitalization of justice has developed steadily in the past decade, with very heterogeneous implementations in the prison institutions of EU member states. Overall, prison services tend not to be first movers in introducing digital technology in detention but rather to react to or follow the digital agenda set by the surrounding society and governmental authorities. Yet, when moves occur, the digital transformation of prison often comes along with managerial or security purposes, or for cost savings reasons. Only in a limited number of countries, digital transformation has been thought as a mean to facilitate the access of the detained persons to their rights.

This paper proposes to analyse the purposes and strategies of digital transformation in prison, to draw an overview of digital initiatives that were implemented in member states and the few legal developments laying the ground for further guarantees on access of the detained persons to digital resources and to the Internet. In conclusion, the paper will underline both risks and opportunities of the reinforcement of access of detainees to digital resources for the access to their rights and to justice.

1. THE FIRST DRIVER OF THE INTRODUCTION OF DIGITAL TECHNOLOGY IN DETENTION: DIGITAL TOOLS TAILORED FOR THE PRISON MANAGEMENT

1.1. Rationalising the management of prison

Digital innovation has offered in recent years new opportunities for prison authorities to transform and improve their prison management systems. With so-called Offender Management Systems going digital, the main aim for the prison administration is to rationalize the prison staff management, improve security and give more autonomy to detainees in certain daily actions, which in end effect would potentially improve relations between prison staff and detainees[1].

Several EU States already partly operated the digitalization of their Offender Management Systems, with basic functionalities such as collection and management of information on detainees relating to their incarceration (initial intake, records of charges, sentencing, temporary release), management of daily life in prison (medical, meal planning, scheduling activities and visits), staff time management.

Private firms offering prison management software offer increasingly news functionalities and modules, such as : digital fingerprinting to identify detainees and increasing accuracy of information on their movements, housing, release ; money deposit and payroll accounting for detainees who work ...[2]

---

[1] See for example the official announcement of the French government plan "Numérique en Détention" in October 2018, https://www.actualitesdudroit.fr/browse/penal/peines-et-droit-penitentiaire/16879/numerique-en-detention-le-futur-outil-pour-ameliorer-les-relations-en-prison

[2] To have an overview of prison digital management systems in EU states, see the report of "ICT in Prison Workshop 2018" of EuroPris network https://www.europris.org/file/report-ict-workshop-stockholm-2018/

At last, an increasing trend in the digital transformation of Justice in Europe is the development of interagency digital cooperation between police, court, prisons and probation, mainly through digitalization of detainees' files and use of cloud services connecting all agencies, with the purpose to speed up procedures.

Several countries, especially in Northern Europe have partly digitalized their systems, several however are far behind, mainly due to lack of strategies, high initial investment costs and rapid outdating of digital systems, or simply lack of expertise.

1.2. Cutting costs in prison budget

Prison administration also look at digital tools as an opportunity to save costs. If overall e-communication such as emailing, video-calling is forbidden or very restricted in most EU states, several States, even the most behind in terms of digital transformation[3] and not surprisingly lower income countries from Southern Europe have experimented video-hearings. This offers surely an opportunity for lawyers and detainees to save their time of transfer to the court when the prison facility is located in another region, but it also obviously saves the costs of transfer to the court (transport and escorting staff costs). In this cost-saving approach, video-hearing should however not substitute but only complement physical attendance at hearings.

Telemedicine is also seen by some states as an opportunity to save costs of staff and transport for the detainee to be transferred to medical facilities. In the USA telemedicine is for example increasingly used for mental healthcare, which in the one hand can make care more accessible in a context of medical staff shortage. On the other hand the quality of care is reduced. In EU States it was experimented for example in Ireland, Austria and Romania. The three latter countries, not only praise telemedicine as a way to reduce costs, but also to reduce security risks due to the transfers of detainees to medical centers. [4]

1.3. Surveillance purposes

Prison administrations have also expanded their use of digital technology to improve prison surveillance systems. From the wide-spread use of video-surveillance, several EU states now look at possibilities given by the use of drones for patrolling inside and outside the penitentiary facilities. Italy or the UK have been for example experimenting such a technology.

Digital technology is also used is several EU States to fight against unauthorized use of cell phones : detect signals of cell phones and jammer communications.

1.4. Increasing self-service of the detained person : a mean for de-escalating frustration and levels of aggression in prison

---

[3]	See for example : the pilot project launched by the newly appointed Secretary General of the Prison Adminisation of Spain on video-conferencing between Bar Associations, prison facilities and courts ; or the legislative decree 123/2018 in Italy forseeing the possibility to participate to surveillance hearing though a videoconferencing.
[4]	http://www.europris.org/file/telemedicine-case-study/

If the rationalization of prison management has been the main driver for digital transformation in prison in the past decade, prison administrations have been recently increasingly engaging in improving the access of detained persons to digital services. Through facilitating access to digital services, prison administrations hope to increase the autonomy of the detained person for the organization of daily life and free prison staff from certain time-consuming tasks. In end effect, prison services also hope for the improvement of relations in prison, the de-escalation of frustrations and levels of aggression by detainees. According to a survey[5] realized in the UK the access of the detained persons to digital services leads to reducing disciplinary offences and reoffending after release. Several prison experts and administrations[6] refer to this survey to argue the need for introducing digital services for the detainees in detention.

2. THE RIGHTS APPROACH : REINFORCING ACCESS TO FUNDAMENTAL RIGHTS OF THE DETAINED PERSONS THROUGH ACCESS TO THE INTERNET AND DIGITAL RESOURCES

Little analysis has been made so far of the potentialities of digital technology for reinforcing access to fundamental rights and access to justice of the detained persons. If a detainee-centered approach is now taking some more importance in digital strategies developed by EU states prison services, especially in Northern European countries, still relatively little case is made of digital resources as key for accessing information, education, but also for accessing the law and justice.

2.1. Digital resources and access to whitelisted Internet websites as a mean to preparation of release

In an effort to improve the rehabilitative dimension of punishment, several EU states have engaged recently in giving the detained persons access to e-learning, online job-search or certain public service websites. Still those services are often reserved to minimum security facilities and not available for detainees in closed facilities.

In Germany, several e-learning projects have been carried out with limited access to the Internet, providing access to courses, information sources, learning programmes, employment related sites. In the case of the E-LIS project, a messaging system and a forum have been integrated, allowing exchanges between students and with teachers under the control of the latter and supervisory agents. Tegel prison also has its own website, created 20 years ago on the director's initiative and entirely created by prisoners where they can tell their daily lives and describe the life in prison. It includes an interactive service and a messaging system, but only a few selected detainees have access to it.

---

[5] Cynthia McDougall, Dominic A. S. Pearson, David J. Torgerson and Maria GarciaReyes, 'The effect of digital technology on prisoner behavior and reoffending: a natural stepped-wedge design', Journal of Experimental Criminology, December 2017, Volume 13, Issue 4, pp455–482.
[6] See Report of EuroPris ICT Workshop in 2019, Sweden https://www.europris.org/file/report-ict-workshop-stockholm-2018/ ; See also official announcement of the French government plan "Numérique en Détention" in October 2018, using the same argument. https://www.actualitesdudroit.fr/browse/penal/peines-et-droit-penitentiaire/16879/numerique-en-detention-le-futur-outil-pour-ameliorer-les-relations-en-prison

In the United Kingdom, several experiments, including e-learning, have been carried out. For example, the Polaris project provides to selected prisoners access to a limited number of sites under the control of an agent. The Virtual Campus project also allows detainees to have access to certain previously controlled sources of information and websites. Detainees can also communicate with their tutors and teachers via secure messaging.

54 of Sweden's 57 prisons are connected to a national e-learning network where they can communicate with their teachers via a virtual forum. In addition, students undertaking higher education can also obtain a network connection, but a teacher must connect at the same time, in order to monitor the nature of the sites they visit.

In the Netherlands, detainees of the so-called reintegration centres have access to a computer. The reintegration centres were created for prisoners to arrange for, *inter alia*, their housing, work or income and identity documents to prepare for their time after the release from prison. In these centres, prisoners can arrange their affairs themselves, working individually on a computer. Prisoners can be assisted during their activities by volunteers and prison workers. In these centres, prisoners have access to the internet, but only certain whitelisted websites are accessible. The prisoner must first discuss the goals for the use of the computer and the necessary websites to that purpose. The use of the computer is supervised. Prisoners in high security regime are excluded from using the facilities in the reintegration centres, as the principle of the centres, is that they are reserved to prisoners who are about to leave prison. Still, as some of the prisoners in the antiterrorist detention regime do not go to another regime before leaving prison, the prison director decided to place a computer on one of the terrorist wings. On this computer, the same possibilities as in the reintegration centre are offered.

In Belgium the Prison Cloud initially offered limited access to internet to whitelisted websites. However the application allowing access to whitelisted websites was withdrawn after an incident in which a detainee managed to send a message to a journalist via a job search page. This was said to be temporary, but up to now, access is still withdrawn.

In Denmark a site for e-learning was set up in the maximum security prisons in 2010, with the ambition to provide the same education solutions as in lower security prisons. Due to the outdating of the software, the systems needs however replacement.

In general, access to the internet, should it be only whitelisted information, education or public services websites, remains very limited in European prisons. Generally authorities put forward three types of arguments to oppose the access to the Internet of detained persons :

- the risks of leakage of sensitive information on prisons and risks of escape
- the maintenance of criminal activities or networks through contacts with the outside world.
- the cost of such access, or its technical impossibility in the case of old facilities

Prison authorities also tend to be careful with experimentations, due to the very recent introduction of digital technologies in prison and the lack of available evaluation and research on results of these experiments.

2.2. Digital technology for maintaining family tights and enabling contact with external intermediates

Besides retrieving information, the use of digital technologies can be used to communicate with legal advisors, and with families, as in the cases of the use of **videoconferences** or Skype or similar software. Skype, however, is impossible to secure. Several field surveys of the EUPRETRIALRIGHTS research project reported how the latter is often mobilized in more or less formal ways by social workers in prison to facilitate communication between prisoners and members of their family who are too far away from the prison to visit, whether they live in remote regions of the country or abroad, as in the case of foreign-national prisoners.

In Ireland, the Prison Service is experimenting a video-conferencing solution which allows video-visits with family, with a special benefit for foreign national detainees. A secure video-link to family/friend of the detainee is emailed to the family, who clicks on it at the designated time. The link is one time only.

In Belgium's Prison Cloud experiment, a videoconferencing system has been developed which is comparable to Skype, but which can be secured. The system meets different goals, by making televisits possible for foreign-national detainees, by providing online consultation between the detainee and the prison personnel, such as social workers and psychologists. It can also make contacts between the lawyers and incarcerated clients possible as well as between the legal authorities and the detainee, and can allow online interrogation and online appearance before court.

In Norway, Skype was introduced as a mean for families to communicate with their relatives in prison. Calls are organized from separate video terminals within the prison with prior whitelisting of the home number of the family to call. The calls are launched, monitored and can be shut down any time by the prison staff. The same type of skype system of calls to relatives is organized in Finland.

The use of such means of communication for virtual family visits or interactions with lawyers or the court[7] raises a series of issues. Some are related to their practical implementation, as several cases of failing technology have been reported. Further, lawyers and other professionals who enter prisons on a regular basis play an important monitoring role. Spreading the use of video-visits at the expense of real visits could lead to a closing off of the prison and hinder public oversight of prison. Finally, besides that virtual visit should only complement and not substitute physical interpersonal interaction and intervention, important safeguards should be developed to insure the privacy of e-communications between prisoners and their families, lawyers or the court.

2.3. Accessing justice

The White Paper on access to justice in pre-trial detention by the research team of the EUpretrialrights project has pointed out that the **legal information** provided in detention is often limited to internal rules and that the obligation to provide legal texts is mainly implemented by making the main penitentiary law and regulatory texts available for

---

[7] Dumoulin, Laurence et Christian Licoppe, *Les audiences à distance. Genèse et institutionalisation d'une innovation dans la justice* : Paris, LGDJ-Lextenso, Coll Droit et Société, 2017

consultation in the library. In practice the necessary texts are often not provided by the prison staff or outdated.

In the countries of the research, the few countries offering digital resources also tend to restrict the type of digital content made available to the detained. In Belgian Prison Cloud, the legal information available on the cloud is mainly restricted to house rules. In the Netherlands, some detainees mention having access to official websites with domestic law and case law in the reintegration centres. Still the authorisation to get access to a specific website is dependant on the prison staff decision in each specific case.

Access to digital services and to the Internet could however represent in this regard a major opportunity for both the detained persons and prison management to organise in an efficient way the actual accessibility to legal texts, for example through accessing domestic law websites or ECtHR case law database or CoE library.

In few countries, **access to lawyer** can also be facilitated through digital technology. As mentioned above the Belgian Prison Cloud enable both the scheduling of a meeting and video-conferencing with the lawyer. In the Netherlands, since September 2018, in two penitentiary institutions lawyers now need to use the application "MyTelio" to arrange a call with their clients, rather than going through the institution. Still using the app involves costs (that previously were not there). The Dutch Bar as well as the NVSA as the NVJSA released statements that they thought using this app would go against the right of clients to freely communicate with their lawyers. There are also concerns whether the confidentiality of the exchange is guaranteed by the system. The Dutch Bar communicated that it had been in consultations with the DJI on the matter, but in the end, the NVSA and the NVJSA, supported by the Dutch Bar, filed an application for a temporary injunction. Pending the proceedings, the obligation to use the app was abolished while the judge urged the parties to resolve the issues. This case is still pending.

Several EU states are in the process of **digitalization of criminal files**. Adding to the facilities provided by "detainees' digital kiosks" such as the Prison Cloud, detainees can potentially have a better and quicker access to their criminal file and this way improve their preparation of their case.

3. EUROPEAN STANDARDS AND NORMS ON ACCESS TO DIGITAL RESOURCES AND TO THE INTERNET IN DETENTION

In recent years, the evolution of the case law of the European Court of Human Rights on prisoners' access to the Internet has provided a solid basis for requiring prisoners to use the Internet to access the kind of documentation to which they are granted access by law.

ECHR case law on prisoners' access to the Internet concerns two cases, Kalda vs Estonia 2016 and Jankovskis vs Lithuania 2017.

Romeo Kalda, a prisoner sentenced to lifetime imprisonment filed a complaint about the authorities' **refusal to grant him access to three internet websites, the website of the Council**

of Europe and two public legal databases hosted on the websites of the Estonian Ministry of Justice and the Estonian Parliament (application no. 17429/10). The applicant, complained in particular that the ban under Estonian law on his access to these specific websites had breached his right to receive information via the Internet and prevented him from carrying out legal research for the court proceedings in which he was engaged. The Court ruled, by six votes to one, that there had been a violation of Article 10 (freedom of expression) of the ECHR. The Court also stated that contracting states are not obliged to grant prisoners an access to the Internet, but pointed to the fact that the Estonian authorities had already made security and budgetary arrangements to grant prisoners the use of Internet via computers specially adapted for that purpose and under the supervision of the prison authorities. The Court stated that if a State is willing to allow prisoners access, it has to specify reasons for refusing access to specific sites. In the specific circumstances of the Kalda case, **the domestic courts had undertaken no detailed analysis of the possible security risks of access to the three websites, which were run by the Council of Europe and by the state itself.** The Court ruled that the security and costs implications of not allowing Kaldas access to the Internet sites in question had not been sufficient to justify the interference with his right to receive information.

Henrikas Jankovskis wished to study law at the University of Vilnius and had written to the Ministry of Education and Science requesting information about the possibility of enrolling in the programme. The Ministry replied that relevant information about study programs could be found on its website, however the prison authorities refused Jankovskis' access to the Internet to view this website. In finding a violation of the applicant's right to receive information, the European Court of Human Rights reasoned that the national authorities had failed to take into account the fact that the Internet access was sought so the prisoner could pursue his education, which was important for his rehabilitation and subsequent reintegration into society. Furthermore, the ECHR was not convinced that sufficient reasons had been put forward to justify the interference with the applicant's right to receive information in this particular case. The European Court of Human Rights found that the interference was not "necessary in a democratic society" and that the Lithuanian authorities had **violated Article 10 of the European Convention on Human Rights by refusing to grant a prisoner access to an Internet website providing education-related information.**

In these two cases, the judgements concern the rights of convicted prisoners to receive information, in Kalda vs. Estonia to carry out legal research, and in the other to seek information that was deemed important for the applicant's rehabilitation and reintegration into society. The access to legal databases through secure Internet connexions raises several issues pertaining **to updated legal material**. Paper versions of legal provisions and case law are circulated more or less formally within prison institutions, but these are often quickly out-dated and sometimes only exist in versions that explain rights rather than make it possible to develop legal strategies.

Similarly, the Council of Europe's Committee for the Prevention of Torture took a position in favour of prisoners' access to the Internet in a report published on 6 September 2018 (CPT/Inf (2018) 41). In this regard, the CPT is the most influential body in terms of producing new standards in prison matters.

CONCLUSION

In conclusion, access to digital resources by the detainees offer several potentialities for both detainees to have a better access to their rights and to justice, and for prison management to facilitate access to legal information and to legal aid to which detainees are granted by law. Still, digital tools and services are often tailor made for the prison administration rather than for the detained persons. Whether for cost-saving or security reasons, the actual services digital tools can offer to the detained persons remain under full control of the prison staff, and worries can be raised, whether the detained persons can get real access to the tools (for example whitelisted vs. blacklisted websites in prison where access to the Internet is made available) or on the contrary can refuse some services (video-hearing or video-visit if physical intervention/meeting is preferred ; or video-conferencing if protection of privacy and confidentiality is not guaranteed)

Internet access and overall access to digital services by detained persons raises in general questions about the potential collection and processing of data for the purpose of assessing behaviors of the detained persons. As the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, points out in a report of 17 April 2013 (A/HRC/23/40), "since the first form of remote communications appeared, States have sought to intercept and monitor private communications for the purposes of law enforcement and national security". Data collection that can "collectively create a profile of an individual's private life, including health status, political and religious opinions and/or affiliation, relationships and interests, revealing as much or even more detail than would be perceptible from the content of communications alone. "

The possibility of using AI in detention context raises the same questions as outside, with "significant concerns, particularly with regard to the origin of data, their accuracy and the rights of individuals with regard to them, the ability of applications to desanonymize their content and the biases they may contain or be instilled when labelled or trained by human operators" or the identification of correlations that are not necessarily cause-and-effect relationships, and [....] can lead to erroneous and biased conclusions that are difficult to verify".

In his report on "Dematerialisation and inequalities of access to public services" of 2019, the French Defender of Rights thus questioned "the consequences that the algorithmic processing of personal data by administrations can have" and the "biased nature of the data used and the discrimination that these technologies can produce", stressing that "the dangers of predictive police or justice software have also been highlighted in the United States".