National report

Jacques, Florian; Mont, Julie; Pielaet, Pierre-Olivier; Degrave, Elise

Published in:
European review of digital administration & law

Publication date:
2021

Document Version
le PDF de l'éditeur

European Review of Digital Administration & Law - Erdal
2021, Volume 2, Issue 2, pp. 231-266
ISSN 2724-5969 - ISBN 979-12-5994-752-9 - DOI 9791259947529 21

National Reports

EUROPEAN UNION

edited by
Andrea CIRCOLO, Ph.D. in EU Law, University of Naples Parthenope
Angelo CORRERA, Ph.D. in EU Law, University of Naples Parthenope

DIGITAL EUROPEAN PROGRAMME

Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 april 2021 establishing the Digital Europe Programme and repealing decision (EU) 2015/2240.

Digital Europe: new funds for technological transformation of enterprises coming soon.

On 11 May 2021, Regulation (EU) 2021/694 of the European Parliament and of the Council establishing the Digital Europe Programme was published in EU Official Journal. Digital Europe has been fine-tuned to support and accelerate digital transformation of Europe's economy, industry and society and to enable citizens, public administrations and businesses to reap its benefits and improve Europe's competitiveness in the global digital economy, helping to reduce the digital divide and enhancing the EU's strategic autonomy through global, cross-sectoral and cross-border support and an increased EU contribution. Investments under the Digital Europe Programme support the Union's two objectives of green transition and digital transformation and strengthen the Union's resilience and strategic autonomy. In particular, with a budget of around € 7.5 billion, the programme finances projects in five key areas, called Specific Objectives, each with defined operational objectives and implementation modalities: supercomputing; artificial intelligence; cyber-security; advanced e-skills; deployment; optimal use of digital capacity and interoperability. In particular:

1. With regard to supercomputing, the programme shall implement the European strategy for HPC by supporting a comprehensive Union ecosystem that provides the necessary HPC and data capabilities for Europe to compete globally. The strategy shall aim to implement a world-class HPC and data infrastructure, thus equipping the Union with its own independent and competitive HPC technology resource to achieve excellence in HPC applications and expand their availability and use. The envisaged operational objectives are:
- to implement, coordinate at EU level and operate an integrated, demand-driven, application-driven, world-class data and supercomputing infrastructure at exascale, easily accessible to public and private users, in particular SMEs, and easily accessible for research purposes;
- implement operational off-the-shelf technologies resulting from research and innovation activities in order to create an integrated Union-wide ecosystem for HPC encompassing various aspects of the scientific and industrial value chain segments, including hardware, software, applications, services, interconnections and e-skills, with a high level of security and data protection;
- implement and operate a post-exascale infrastructure, including integration with quantum computing technologies, and research infrastructures in the field of computing; encourage the development in the EU of the necessary hardware and software for such implementation.

Actions under this Specific Objective shall be implemented primarily through the European High Performance Computing Joint Undertaking established by Regulation (EU) 2018/1488.

2. With regard to Artificial Intelligence (AI), on other hand, the programme develops and strengthens core AI capabilities in Europe, including data resources and algorithm repositories and makes them accessible to businesses and public administrations, and strengthens and networks existing or newly established AI testing and experimentation facilities in the Member States.

Operational objectives, in this case, are to:
- develop and enhance the AI capabilities and knowledge base in the EU and the algorithm repositories, ensuring a people-centred and inclusive approach that respects EU values;
- make the above capabilities accessible to businesses (in particular SMEs and start-ups), civil society, non-profit organisations, research institutes, universities and PAs, in order to maximise their benefits to society and the economy;
- strengthen and network testing and experimentation facilities for AI in the Member States;
- develop and enhance commercial application and production systems in order to facilitate the

integration of technologies into value chains and development of innovative business models; can reduce time gap between innovation and its commercial exploitation and foster the uptake of AI-based solutions in areas of public interest and society.

AI-based solutions and the data made available must respect the principle of privacy and security by design and comply with data protection legislation. Actions under this Specific Objective shall be implemented mainly through direct management.

With regard to Artificial Intelligence (AI), on the other hand, programme develops and strengthens core AI capabilities in Europe, including data resources and algorithm repositories and makes them accessible to businesses and public administrations, and strengthens and networks existing or newly established AI testing and experimentation facilities in Member States.

The operational objectives, in this case, are to:
- develop and enhance AI capabilities and knowledge base in the EU and the algorithm repositories, ensuring a people-centred and inclusive approach that respects EU values;
- make the above capabilities accessible to businesses (in particular SMEs and start-ups), civil society, non-profit organisations, research institutes, universities and PAs, in order to maximise their benefits to society and the economy
- strengthen and network testing and experimentation facilities for AI in the Member States;
- develop and enhance commercial application and production systems in order to facilitate the integration of technologies into value chains and development of innovative business models; reduce time gap between innovation and its commercial exploitation and foster the uptake of AI-based solutions in areas of public interest and society.

AI-based solutions and the data made available must respect the principle of privacy and security by design and comply with data protection legislation. Actions under this Specific Objective shall be implemented must be improved with a cross-cutting and direct approach. Through the cyber security and trust objective, the programme shall foster the strengthening, development and acquisition of key capabilities aimed at securing the EU's digital economy, society and democracy, enhancing its industrial potential and competitiveness in the field of cyber security, as well as improving capacities to protect citizens and businesses against cyber threats.

The Regulation provides for following operational objectives:
- to support the development and procurement of equipment, data infrastructures and advanced tools for cybersecurity, together with Member States, in order to achieve a high common European level of cybersecurity, while respecting data protection law and fundamental rights and ensuring EU strategic autonomy;
- to support the development and optimal use of European knowledge, capabilities and expertise related to cyber security, as well as the sharing and integration of best practices;
- ensure wide deployment of effective and state-of-the-art cyber security solutions across all economic sectors, with a particular focus on public authorities and SMEs;
- strengthen the capacities of Member States and the private sector to help them comply with Directive (EU) 2016/1148 including through measures to support the adoption of best practices in cybersecurity;
- improve resilience to cyber attacks, contribute to developing greater risk awareness and better knowledge of cyber security processes, support public and private organisations in achieving basic levels of cyber security;
- improving cooperation between the civil and defence sectors on cyber security projects, services, expertise and dual-use applications.

Actions under this Specific Objective shall be implemented primarily through the European Centre of Expertise in Cyber Security Industry, Technology and Research and its network of National Coordination Centres.

4. In a context of advanced e-skills, programme can contribute to widening EU talent pool, bridging the digital divide and fostering greater professionalism, in particular in high performance and cloud computing, Big Data analytics, cyber security and distributed ledger technologies (e.g. blockchain, quantum technologies, robotics, AI).

In order to address skills supply/demand mismatches and encourage specialisation in digital technologies and applications, financial support will be provided to:
- support the design and delivery of high-quality long-term (including blended learning for students and the workforce) and short-term training courses and activities for the workforce, in particular in SMEs and the public sector
- support high-quality on-the-job training activities and work experience for students (including work placements) and the workforce, particularly in SMEs and the public sector.

5. Finally, with regard to the implementation

and optimal use of digital capabilities and interoperability, the new Regulation foresees the objective of supporting the public sector and the sectors of public interest (health and care, education, justice, customs, transport, mobility, energy, environment and the cultural and creative sectors, including their businesses) to implement and effectively access state-of-the-art digital technologies, such as HPC, AI and cybersecurity; implement, operate and maintain state-of-the-art interoperable digital infrastructures and services at trans-European level, in a complementary way to national and regional actions; support the integration and use of trans-European digital service infrastructures and approved European digital standards in the public sector and areas of public interest to facilitate cost-effective implementation and interoperability; facilitate the development, upgrading and use of solutions and frameworks by public administrations, businesses and citizens, including open source solutions and reuse of solutions and frameworks for interoperability; enable the EU public sector and industry, in particular SMEs, to have easy access to piloting and testing of digital technologies and to expand their use also across borders; support the take-up by the public sector and industry (in particular SMEs and start-ups), of advanced and related digital technologies, including in particular HPC, AI, cyber security, other state-of-the-art and future technologies such as distributed ledger technologies; support the design, testing, deployment and maintenance of interoperable digital solutions, including digital PA solutions, for EU-wide public services delivered through a data-driven reusable solutions platform aimed at fostering innovation and establishing common frameworks to realise the full potential of PA services for citizens and businesses; ensure continued capacity at EU level to lead digital development, as well as to observe, analyse and adapt to rapidly evolving digital trends and share and integrate best practices; support collaboration on the establishment of a European ecosystem for trusted digital data sharing infrastructures using services and applications based on distributed ledger technologies (e.g. blockchain), including supporting interoperability and standardisation and promoting the deployment of EU cross-border applications based on security and privacy by design, respecting consumer and data protection legislation; implementing and enhancing European Digital Innovation Poles and their networks.

The programme is implemented partly under direct management and partly indirectly. It can provide funding in the form of procurement (main form), grants and prizes or in the form of financial instruments (as part of mixed financing operations). It can also be implemented through European partnerships. For the implementation of the programme, the Commission adopts work programmes, with an indicative duration of two years for the specific objectives of IA, deployment and optimal use of digital capacity and interoperability and for any other actions under the direct management of the specific objectives of supercomputing and cyber-security. The work provides for the identification of individual actions for improvement, the amounts set and, where appropriate, the conditions to be met, including the eligible states (in fact, not all contracts/subsidies will be open to eligible third countries and eligibility may be limited to EU states when there are even potential security problems). Within the program first year, a European network of Digital Innovation Poles will be set up, comprising in principle at least one pole per Member State. A European Digital Innovation Cluster is a legal entity that provides (even indirectly) access to technological expertise and testing facilities (e.g. equipment and software tools), with the aim of enabling digital transformation of industry and facilitating access to finance. It is open to enterprises of all shapes and sizes, in particular SMEs, mid-cap companies and scale-ups, as well as EU public administrations. In implementing programme, European Digital Innovation Poles carry out a range of activities for the benefit of EU industry (especially SMEs and mid-cap companies) and the public sector, and in particular they work on:

- (a) raising awareness and providing expertise, know-how and services for digital transformation, including testing and experimentation facilities, or ensuring access to them;
- assisting enterprises, organisations and public administrations to become more competitive and improve their business models through the use of new technologies;
- facilitate the transfer of skills and know-how between regions, in particular by linking SMEs, start-ups and mid-cap companies in one region with European digital innovation poles in other regions that can best provide the services required; encourage exchanges of experience and expertise, joint initiatives and good practice
- provide thematic services, in particular those related to AI, HPC and cyber security and trust, or ensure access to them by public administrations, public sector organisations, SMEs or mid-cap companies;

- provide financial support to third parties.

EIPs may specialise in certain thematic services and are not obliged to provide them all or to all categories of stakeholders. Potential candidates for membership of the EIP network are nominated by each Member State through an open and competitive procedure (according to criteria set by the Commission) and then selected by Commission on the basis of additional criteria. Additional clusters may subsequently be selected in order to meet the demand for their services in all regions of the EU, including the outermost regions. A pole may receive funding from the programme in the form of grants.

The Regulation entered into force on 11 May 2021 and applies from 1 January 2021.

PATH TO THE DIGITAL DECADE

Proposal for a Decision of the European Parliament and of the Council establishing the 2030 policy programme "Path to the Digital Decade" of 15 September 2021, COM (2021) 574 final.

Commission presents a "Path to the Digital Decade".

On 15 September 2021, the European Commission presented its proposal for a concrete plan to achieve the digital transformation of the EU society and economy by 2030. The aim of the plan is to establish a governance framework based on an annual cooperation mechanism with member states and aimed at achieving the 2030 Digital Decade objectives at EU level in the areas of e-skills, digital infrastructure and digitisation of businesses and public services. In Article 2 of the proposed plan, the Commission has, in particular, reiterated that the objectives to be achieved jointly with the Member States include promoting an open, people-centred digital environment, characterised by digital technologies and services in line with the principles and values of the Union, and strengthening the collective resilience of the Member States, ensuring a secure digital infrastructure with high standards of privacy, in which public services and health and welfare services are accessible online for all.

Building on the Digital Compass 2030, the Commission has outlined the above-mentioned annual cooperation mechanism with Member States through the following instruments:
- a structured, transparent and shared monitoring system based on the Digitisation of Economy and Society Index (DESI) to measure progress towards each of the 2030 targets;
- an annual 'State of the Digital Decade' report, in which the Commission will assess progress and recommend possible actions;
- multi-annual strategic roadmaps for the Digital Decade for each Member State, in which Member States will outline the policies and measures adopted or planned in support of the 2030 targets;
- an annual structured framework to discuss and address areas of insufficient progress, with joint recommendations and commitments between the Commission and Member States;
- a mechanism to support the implementation of multi-country projects.

ARTIFICIAL INTELLIGENCE IN EDUCATION, CULTURE AND THE AUDIOVISUAL SECTOR

European Parliament Resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector (2020/2017(INI)).

AI for sustainable development of education, culture and the media sector.

On 19 May 2021, the Parliament adopted a resolution on the use of AI in education, culture and the audiovisual sector, stressing, inter alia, that AI technologies must be used in all areas of life.

While it is easy to understand the potential effects of AI in sectors such as telecommunications, transport, traffic management or health, assessing its long-term impact on education, culture and the audiovisual sector is much more complex. Despite the consensus view that AI and automation are likely to help create more wealth and simplify many processes, the use of AI has also raised deep concerns about a possible increase in inequality, discrimination and unemployment.

The potential impact of AI on education, culture and the audiovisual sector is rarely addressed and remains largely unknown. However, it is a matter of fundamental importance, as AI is already being used in education as well as in the production of films, songs, stories and paintings.

This resolution therefore aims to foster a concrete understanding of the current impact of AI in these areas as well as the impact of future technological advances over the next decade. In particular, the resolution focuses on how AI can transform these sectors and the specific regulatory challenges that the Union may face in this respect. With reference to the education sector, the resolution underlines that artificial intelligence has many applications, such as customisable ap-

proaches to learning, AI-based tutors, textbooks and teaching materials with personalised content, intelligent algorithms to determine the best teaching methods, AI-based game engines and adaptive user models in personalised learning environments (PLEs) that can enable early detection of difficulties, such as dyslexia or school drop-out risks.

Personalized learning experience that the use of artificial intelligence enables in education would allow students to enjoy an educational approach fully adapted to their individual abilities, needs and difficulties, allowing teachers to closely monitor students' progress. However, to make personalised education a reality, large amounts of personal data need to be collected, used and analysed. In this respect, the current lack of access to personal data on students risks impeding the effective implementation of AI in education. It is therefore essential to ensure the security and transparency of the collection, use, management and dissemination of personal data, while safeguarding the confidentiality and privacy of learners' personal data. Furthermore, addressing the risks of potential AI distortions and addressing the issue of data storage should be a priority in any initiative for the broad deployment of AI in the education system at Union level.

But AI has also become increasingly important for cultural heritage, particularly in response to potential modern threats such as climate change or conflict. AI can have several applications in this respect: it can be used to improve user experience by allowing visitors to cultural institutions and museums to create personal narrative paths or to use virtual tour guides. Conversational robots could communicate interactively about cultural heritage on any topic and in any language. They would also facilitate access to information while providing a vivid cultural experience to users.

The resolution also underlines how AI is changing the way cultural and creative industries, in particular the audiovisual sector, work. In this field, there are already multiple applications, such as data-driven marketing and advertising, training machine learning algorithms to develop promotional film trailers and design advertisements; personalisation of the user experience, using machine learning to recommend personalised content based on user activity and behaviour data, search optimisation, etc. Although AI offers a wide range of opportunities in the production of high-quality cultural and creative content, centralised distribution and access to such content raises a number of ethical and legal issues, in particular with regard to data protection, freedom of expression and cultural diversity. Indeed, the criteria used to select or recommend a work on the major platforms are neither transparent nor verifiable and may be decided on the basis of economic factors that exclusively benefit these platforms.

Issue of cultural and linguistic diversity in recommendation systems is therefore crucial and needs to be addressed. Rapporteur stresses the need to establish a clear legal framework for transparent, accountable and inclusive algorithms in order to safeguard and promote cultural and linguistic diversity.

The regulatory challenges posed by AI applications in the audiovisual sector are also linked to existing legal acts, such as the AVMSD. Therefore, a more in-depth assessment of the urgency and/or political momentum for future adaptations of these files to AI may be needed.

Although AI can help empower many creators, making CCS more prosperous and promoting cultural diversity, the vast majority of artists and entrepreneurs may not yet be familiar with AI tools.

There is a lack of technical knowledge among creators that prevents them from experimenting with machine learning and reaping the benefits it can bring. Therefore, it is essential to assess what skills would be needed in the near future, while improving training systems, including upskilling and reskilling, ensuring lifelong learning throughout working life and beyond.

In this context, the European Parliament suggests setting up an AI observatory with the aim of harmonising and facilitating evidence-based monitoring of new AI developments in order to address the issue of verifiability and accountability of AI applications in CCS.

ARTIFICIAL INTELLIGENCE AND CRIMINAL LAW

European Parliament Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)).

Artificial intelligence: European Parliament calls for strict rules on criminal applications.

On 6 October 2021, the European Parliament adopted a resolution on Artificial Intelligence (AI) in criminal law and its use by police and judicial authorities in criminal matters. The increasing use of AI in criminal law is based, in

particular, on the promise that it will improve the prevention and law enforcement of certain types of crimes (among which financial crimes, money laundering, terrorist financing, sexual abuse and sexual exploitation of children online as well as certain types of cybercrimes are mentioned in the Parliament's resolution) and facilitate more objective decision-making.

Although European Parliament recognises positive contribution of certain types of AI applications to law enforcement and judicial authorities across EU, it notes in this resolution the potential risk of such tools for the protection of fundamental rights, making a number of recommendations. Among these, it is highlighted that the AI systems, in order to guarantee their security and legitimacy, must be programmed, produced and used according to the principles of transparency, explainability, non-discrimination, contestability and traceability of the processes and results achieved. These principles go hand in hand with the concept of human-centric AI, according to which AI systems should be designed in such a way that they can always be deactivated by a human operator.

Parliament points out that the use of AI applications by police and law enforcement authorities should be classified as high risk. In addition, its development, deployment and use should be subject to continuous risk assessment and a rigorous test of necessity and proportionality. Instead, it recommends an explicit ban on certain uses of AI systems, such as those that could result in mass surveillance, harm the physical integrity of human beings, confer rights or impose legal obligations on individuals, as well as the use of AI and related technologies for judicial decision-making. Finally, the Parliament calls for a ban on the use of private facial recognition databases for law enforcement purposes.

It calls for a consistent application of the precautionary principle for all AI applications in the context of law enforcement, emphasising that legal responsibility and accountability must always lie with an identified natural or legal person for decisions made with the support of AI.

With regard to certain specific applications, the Parliament highlights that the use of techniques of so-called predictive policing, if on the one side allows the analysis of the data sets supplied for the identification of models and correlations, on the other side, cannot give an answer to the question of causality, cannot make reliable forecasts on the behaviour of individuals and, therefore, cannot constitute the sole basis for intervention.

EU RIGHT TO DISCONNECT

European Parliament Resolution of 21 January 2021 with recommendations to the Commission on the right to disconnect (2019/2181(INL)).

Right to disconnect: towards a definition of a new EU fundamental right.

On 21 January 2021, the European Parliament adopted a resolution concerning recommendations to the European Commission on the proposal for a directive on the right to disconnect through the introduction of an objective and reliable system for measuring daily working time in a way that respects workers' right to privacy and the protection of personal data.

The European Parliament initially stressed that the measures taken as a result of the COVID-19 crisis have changed way people work and have demonstrated importance of digital solutions, including use of teleworking schemes by enterprises and public administration bodies across the Union.

However, the increasing use of digital tools for work purposes has led to the emergence of an 'always on', 'always online' or 'always on call' culture which can be detrimental to workers' fundamental rights and fair working conditions, including fair pay, working time limits and work-life balance, physical and mental health, occupational safety and well-being.

As the right to disconnection is a fundamental right that is an inseparable part of the new working patterns of the new digital era, but there is currently no specific EU legislation on the right of workers to disconnect from digital tools, including information and communication technologies (ICT), for work purposes, the Parliament called on the Commission to to put forward, on the basis of a thorough assessment, a proper evaluation and a consultation of Member States and the social partners, a proposal for a Union directive on minimum standards and conditions to ensure that workers are able to exercise effectively their right to disconnect and to regulate the use of existing and new digital tools for work purposes, whilst taking into consideration the European Social Partners Framework Agreement on Digitalisation, which includes arrangements for connecting and disconnecting' (para 13).

In particular, according to the Parliament, such a proposal would have to take into account a number of factors and to impose some obligations, including:

- being constantly connected, together with the

high demands at work and the increasing expectation that workers can be reached at any time, can negatively affect workers' fundamental rights, their work-life balance, as well as their physical and mental health and well-being. For this reason, it is important to implement psychosocial risk assessments at the level of public and private enterprises;
- employers should not require workers to be directly or indirectly available or reachable outside working hours and that workers should refrain from contacting colleagues for work purposes outside agreed working hours; recalls that periods during which the worker is available or reachable for the employer are working periods;
- workers exercising their rights under the Directive should be protected against any adverse consequences, including dismissal and other retaliatory measures. Such workers should also be protected against any discriminatory measures, such as loss of income or promotion opportunities. They should also have adequate and rapid judicial and administrative protection against any adverse treatment in response to the exercise of their rights under the Directive or to an attempt to exercise them, including the right of appeal and the right to institute administrative or judicial proceedings to ensure compliance with the Directive;
- member States should actively support and encourage right to disconnection and promote an efficient, reasoned and balanced approach to digital tools at work, as well as awareness-raising measures and information and training campaigns on working time and the right to disconnect (e.g., through national labour inspectorates, Member States should check that employers provide workers with a statement setting out these practical arrangements);
- social parties should be involved in order to ensure effective enforcement of the right to disconnect, in accordance with national practices, including through the conclusion of collective agreements within each Member State; these would help to define the practical arrangements for the exercise of the right to disconnect by the workers and for the implementation of this right by the employer.

The Commission's proposal for a directive is expected in 2022. It is hoped that the legislative procedure will be 'fast-tracked'. Remote working has enormously grown in the recent months, but only four Member States currently recognise a right to disconnection in their legislation (Belgium, France, Italy and Spain).

CONSUMER PROTECTION ASSOCIATIONS AND REPRESENTATIVE ACTIONS AGAINST INFRINGEMENTS OF THE PROTECTION OF PERSONAL DATA

Advocate General Richard de la Tour's Opinion in Case C-319/20, Facebook Ireland Limited v. Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. (request for a preliminary ruling from the Bundesgerichtshof - Federal Court of Justice, German), delivered on 2 December 2021.

According to Advocate General Richard de la Tour, the Member States may allow consumer protection associations to bring representative actions against infringements of the protection of personal data. Those actions must be based on infringements of rights which the data subjects derive directly from the General Data Protection Regulation (GDPR).

In Germany, Federal Union of Consumer Organisations and Associations accused Facebook of infringing data protection rules in connection with the offer of free games provided by third parties on the platform. In that context, Federal Union brought an action for an injunction against Facebook Ireland before the German courts.

According to the *Bundesgerichtshof* (Federal Court of Justice, Germany), Facebook did not provide users with the necessary information regarding the purpose of data processing and data recipient, thus violating General Data Protection Regulation (GDPR).

Doubts, however, arise as to the admissibility of the application. The German court questioned whether an association of interests such as the applicant is entitled to bring an action for protection of the Regulation, irrespective of whether the data subjects' rights have been concretely infringed and in the absence of a mandate from the data subjects.

The *Bundesgerichtshof* therefore asked the Court of Justice to give an interpretation of the GDPR.

In his Opinion, Advocate General Jean Richard de la Tour suggested that the Court should interpret the General Data Protection Regulation as meaning that it does not preclude national legislation which allows associations for the protection of consumer interests to bring legal proceedings against the alleged perpetrator of an infringement of the protection of personal data, if representative action at issue seeks to ob-

tain respect for rights which the persons subject to the contested processing derive directly from that Regulation.

The Advocate General recalled that, in his judgment in *Fashion ID* (29 July 2019, Case C-40/17), the Court had ruled, with reference to Directive 95/46 4 which preceded the General Data Protection Regulation, on a similar question. It thus ruled that that directive does not preclude national legislation which allows associations for the protection of consumer interests to bring legal proceedings against the alleged perpetrator of an infringement of the protection of personal data.

The Advocate General considers that neither the replacement of Directive 95/46 by a regulation nor the fact that the General Data Protection Regulation now devotes an article to the representation of data subjects in legal proceedings can call into question the findings of the Court in that judgment. Therefore, in his view, the Member States are still entitled to provide that certain entities may, without a mandate from the data subjects and without the need to rely in court on the existence of specific cases concerning individually designated persons, bring representative actions aimed at protecting the collective interests of consumers, where it is alleged that Regulation in question conferring subjective rights on data subjects have been infringed. That is precisely the case with the action for an injunction brought by the Federal Union against Facebook Ireland.

Furthermore, the Advocate General considers that the GDPR does not preclude national provisions authorising an association for the protection of consumer interests to bring an action for an injunction in order to ensure respect for the rights conferred by that Regulation by means of rules intended to protect consumers or to combat unfair commercial practices. Those rules may in fact include provisions similar to those contained in that Regulation, in particular as regards information to data subjects concerning the processing of their personal data, which means that the infringement of a rule on the protection of personal data may at the same time constitute an infringement of rules concerning consumer protection or unfair commercial practices.

According to the Advocate General, the defence of the collective interests of consumers by associations is particularly suited to the attainment of the objective of establishing a high level of protection of personal data.

ARTIFICIAL INTELLIGENCE IN JUDICIAL SYSTEMS

Council of Europe, European Commission for the efficiency of Justice (CEPEJ) Revised roadmap for ensuring an appropriate follow-up of the CEPEJ Ethical Charter on the use of artificial intelligence in judicial systems and their environment - Document adopted at the 37th plenary meeting of the CEPEJ, 8 and 9 December 2021, (CEPEJ(2021)16).

AI in judicial systems: new action plan on digitalisation for a better justice.

On 8 and 9 December 2021, the European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe adopted an action plan on digitisation for better justice for 2022-2025 , with the aim of reconciling the efficiency of new technologies and respect for fundamental rights. Technology has played a key role in creating a fundamental basis for the adoption of AI. The digitisation of court systems in different jurisdictions can be cited as the most widespread use of technology. The process of digitisation of courts began at the end of the third industrial revolution. Now, the information technology revolution offers an excellent opportunity to transform the court system into an extraordinarily fast, efficient and high-quality range of services available to all citizens and residents. The digitisation of justice systems creates a fundamental basis on which to use available data to identify areas of the justice system where the application of AI can have a significant impact.

The introduction of AI within justice framework can promise to improve procedural and administrative efficiency, aid in decision-making by judges, lawyers and litigants, and further predict outcomes consistent with past precedents. We must, however, also consider ethical challenges that AI use presents, especially in case of automated decision-making. Transparency and explainability are important where AI-based technologies are adopted. Lack of transparency regarding the algorithms used, often due to legal protection of trade secrets, risks undermining the rule of law. “The principle of the rule of law requires that rules be publicly stated with prospective application and possess the characteristics of generality, equality and certainty. An important procedural dimension of the rule of law is the effective ability to challenge decisions. The failure of users to understand algorithms because they are not trained to understand the

technicalities of the systems creates a situation that risks being detrimental to the justice system. Most users are not trained to understand algorithms and relevant operations, which leads to a situation where the creators of artificial intelligence solutions have more information than the users of artificial intelligence solutions. It becomes difficult to identify possible biases that would affect the outcome of cases and the lack of knowledge of the inputs and outputs that facilitate the operation of the system undermines the judicial norm of reasoned orders. The use of AI in a public institution, such as the judiciary, must be aware of pre-existing and inextricable social contexts and the dynamics that affect them. The EU, through European Commission for the Efficiency of Justice (CEPEJ), has adopted the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. 16The Charter was developed for public and private stakeholders responsible for the design and implementation of artificial intelligence tools and services involving the processing of judicial decisions and data. The Charter introduced five principles to be considered in the use of AI in judicial systems and their environment: respect for fundamental rights; non-discrimination; quality and security; transparency, impartiality and fairness; and 'under the control of the user'. It identifies the uses of AI in the judicial systems of EU Member States and presents an overview of the importance of open data policies related to judicial decisions in the judicial systems of EU Member States. The Charter also touches on AI and legal reasoning; how AI can be applied in civil, commercial and administrative justice; the protection of personal data; and the potential limits of predictive justice tools. In addition, the Charter also specifies the uses of AI in European justice systems that can be encouraged.

In order to fulfil its mission as guarantor of human rights and protection of individuals, the CEPEJ with its recent document dictated a revised roadmap for the creation of a labelling/certification body for artificial intelligence systems and tools used in the field of justice, as a logical follow-up to the CEPEJ's European Ethical Charter on the use of artificial intelligence in justice systems and their environment adopted in 2018.

In particular, the action plan defines the main guidelines of the CEPEJ, whose main objective is always to put the user at the centre of concerns, including in a digitised environment or in the course of digitisation, providing the user with an effective and quality public service of justice. These guidelines are in fact articulated around major axes that aim to ensure that justice is always transparent, collaborative, humane, people-centred and accessible, enlightened and finally accountable and responsive. The future work of the CEPEJ will have to take into account, for the next four years, one or more of these requirements.

In light of the circumstance that the development of information technologies and the integration of artificial intelligence in judicial systems are now an integral part of current justice reforms in many Council of Europe member states, the CEPEJ particularly wishes to recall, through this instrument, its essential role in the protection of human rights and the protection of individuals.

In the same vein, the CEPEJ has just adopted its Guidelines on electronic judicial filing (e-filing) and the digitisation of courts, the revised SATURN Guidelines for the management of judicial time and its programme of activities for 2022 and 2023.

BELGIUM

edited by
Elise DEGRAVE, Professor at University of Namur. Director of investigation of NADI-CRIDS
Florian JACQUES, Teaching assistant at University of Namur and researcher at NADI-CRIDS
Julie MONT, Teaching assistant at University of Namur, researcher at NADI-CRIDS and lawyer at Namur Bar
Pierre-Olivier PIELAET, teaching assistant at University of Namur, researcher at NADI-CRIDS and lawyer at Walloon Brabant Bar

TRANSMISSION OF PERSONAL DATA BY PUBLIC AUTHORITIES

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 72/2021 of 14 June 2021.

The BDPA examined a complaint from the director of a non-profit association that had been the subject of an internal audit, and whose salary data had been communicated to the trade union representatives when the audit report was transmitted.

In order to justify the disclosure of the salary data of its director, the non-profit association

argued that the director was the subject of a complaint. Thus, under its privacy policy, it was allowed to transfer data to third parties for the sake of the investigation of the case. The non-profit association stated that the processing was based on Articles 6.1.d) and 6.1.e) of GDPR. The litigation chamber confirms that the association, as regional public authority in charge of social action, can base its processing on article 6.1.e) of GDPR. However, the BDPA considered that although the non-profit association did have a legal basis in national law, the processing itself was not necessary for exercise of relevant public authority, as it could simply inform the trade union representatives of the outcome of the complaint, without sending them the audit report. The authority also rejected Article 6.1.d) of GDPR as a basis for processing because the purpose of the processing was to assist in the resolution of a social conflict. The applicant also claimed further processing of his data, as the union representatives had forwarded the report to colleagues, who in turn forwarded it to non-profit association's staff. However, the BDPA rejected this argument due to lack of evidences. Finally, the litigation chamber found that the non-profit association had violated Articles 15.1, 12.3 and 13.1.c of GDPR by failing to respond to the complainant's request for access within the time limit. The authority reprimands the non-profit association for violations of the right of access and Article 6.1.e) of GDPR.

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 55/2021 of 22 April 2021.

Another complaint against a public institution for refusal to erase and breach of confidentiality in the processing of a file was submitted to the BDPA.

The father of a child being followed by a childcare institution filed a complaint against the institution on the grounds that it (1) transferred confidential information to the child's mother (who used it in the context of their divorce proceedings), and (2) it failed to responded to his request for erasure. In the course of the proceedings, the complainant also argued that the data processing carried out by the institution was illegal. The Authority notes that the institution intervenes, within the framework of its legal mission, in family situations in order to provide specialised assistance and thus performs a mission of public interest enshrined in Belgian law. However, the BDPA states that the institution cannot rely on Article 6.1.e) of GDPR because the processing legal basis (i.e. a decree under national law) is not sufficiently predictable. Furthermore, the authority finds that the complainant was not sufficiently informed of the identity of the institution's DPO. Hence a violation of Articles 13.1.a) and b) of GDPR was established. With regard to the confidentiality of the data transmitted by the institution to the child's mother by e-mail, the litigation chamber considers it as a violation of Article 25.1 and 25.2 of GDPR. According to the BDPA, the institution failed to implement the technical and organizational measures to ensure the respect of the rights of the data subjects or to limit the accessibility of the personal data. The Authority issues a reprimand for the violations of Articles 13.1.a) and b) and 25.1 and 25.2 of GDPR. It closes the complaint for the rest, and in particular for the violation of the right to erasure invoked by the father of the child, concerning his own data but also those of his son. The authority considers that the deletion of the data would indeed greatly harm the institution's ability to carry out its mission correctly, especially if it is seized again of a file concerning this family in the future.

ACCESS TO AND USE OF PERSONAL DATA FROM NATIONAL DATABASES

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 56/2021 of 26 April 2021.

A woman filed a complaint against a bank which, through the intermediary of an employee who is the ex-husband of the complainant, consulted 20 times her financial data as registered at the National Bank of Belgium (central credit register).

The claimant alleges that her ex-husband used her financial data in the context of their divorce proceedings. Although it accepts that the complainant's ex-husband should be considered as the controller of the abusive consultations, the litigation chamber considers that it was the bank's responsibility to implement technical and organisational measures to avoid abusive data processing by its employees, especially in the case of particularly sensitive financial data. The BDPA recalls that it recommends to implement and keep log files. In this case, the bank did have an access log for non-executive employees, but not for executive employees. The DPA considers this as a flagrant violation of Article 32 of GDPR, which requires that security of processing operations. Since the bank is not able to provide information to the complainant about da-

ta consulted, the chamber also concludes that the bank failed in its duty to inform (article 14.3. of GDPR) and does not respect the complainant's right of access (article 15 of GDPR). On the other hand, the authority rejected the complainant's argument that the bank's DPO did not meet the independence requirement (Article 38 of GDPR), on the grounds that the DPO also acted as CISO (Chief Information Security Officer). The bank was ordered to bring access to the National Bank's register by its senior employees into compliance with GDPR within three months, and to pay an administrative fine of 100,000 euros.

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 129/2021 of 26 November 2021.

The BDPA ruled on a complaint regarding access to the database of the National Register by a municipal employee.

In this case, claimant discovered that his sister-in-law had accessed to National Register database in connection with a family dispute. He therefore brought an action against the municipality in which his sister-in-law was employed. It emerged from the proceedings that his sister-in-law had asked one of her colleagues to access to the National Register in order to obtain information about the claimant. In substance, the BDPA found that, although the proceedings were directed against the municipality, the claimant's sister-in-law could have took part to the proceedings. She could have been considered as the data controller, since the consultation carried out was of a private nature and therefore unrelated to the data processing carried out by the municipality. The litigation chamber considered that the processing had no legal basis, as it was not related to the public interest mission of the municipality. Finally, the BDPA considered that the municipality had violated the principle of data security because it did not have a daily consultation register of the database of the National Register, which would have made it possible to control the consultations carried out. Since Belgian law does not enable to fine a public authority, the municipality received a reprimand and an order to bring its processing activities in compliance with GDPR.

DATA PROCESSING BY TAX AUTHORITIES

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 66/2021 of 4 June 2021.

The BDPA received a complaint after a refusal from the tax authorities, among other things, to rectify personal data whose accuracy was contested by the data subject.

In this dispute, the applicant discovered she was mentioned as "potential figurehead" in relation to investigation opened by the defendant (SPF Finance) against other taxpayers. Therefore, she filled requests to exert her rights to information, access, rectification and limitation of the processing. The defendant refused the request of the applicant on three grounds. First, according to the SPF, the words "potential figurehead" were not personal data under GDPR. Thus, rights to rectification and restriction of processing were not applicable to this information. The BDPA recalled that, subjective assessments fall under the notion of personal data in particular when being combined to the applicant's name and national number. Second, the defendant held that the applicant had already access to her administrative file on the basis of administrative transparency requirements. Nevertheless, DPA found that compliance with this requirement does not relieve the data controller of its duty to respond timely to requests of data subjects. Third, the SPF argued that it was entitled to restrict, partially or totally, the applicant's rights in application of the Act of 3 August 2012 due to a risk of collusion with third parties subject to tax investigation. The BDPA however held that such limitations were only permitted if the data subject faces itself tax investigation. In addition, the restriction should be terminated after a time period of one year after introduction of a data subject request to exerts rights granted under GDPR. Since the defendant was not subject of an investigation and more than a year had elapsed at the time of the BDPA's decision, a breach of the Act of 3 August 2012 on data processing by SPF Finance and of articles 12.3, 12.4, 14, 15, 16, 18 of GDPR was established. Finally, the BDPA found that, in violation of the Act of 3 August 2012, the defendant failed to inform the applicant when limitation to her rights ended. Therefore, a breach on the requirement to facilitate data subject rights was also established. Consequently, the authority issued a reprimand, ordered to comply with data subject's requests and ordered to inform any data recipient of the rectification request.

Brussels Court of Appeal, Brussels Markets Court, 19th Chamber A, judgment of 1 December 2021.

Appeal against the aforementioned decision

of the litigation chamber of the Data Protection Authority 66/2021 of 1st December 2021 before Brussels Markets Court. The Court annulled the BDPA's decision.

The Court found that the decision of the litigation chamber had to be annulled since it was violating the precautionary principle and the obligation to provide the grounds of the decision. First, as pointed out by the SPF Finance (i.e. the appealing party), the claimant before the BDPA tried to use her right to lodge a complaint with the supervisory authority for other purposes than ensuring her right to data protection. In the case at hand, the Markets Court highlighted that an intention to use the right of information in order to know each tax investigation files where she was mentioned as "potential figurehead" can be clearly identified in the data subject complaint. Therefore, such "phishing expedition" constitutes an abuse of right to lodge a complaint (i.e. using the right to lodge a complaint in order to obtain (1) tax information that might lead to prosecution of tax offence and (2) erasure of this information). As the Court recalled, article 54 of the EU charter of fundamental right prohibits the abuse of rights when exercising the rights enshrined in it (including right to data protection of article 8). In application of the precautionary principle, the BDPA had therefore to verify the applicant's true intent during the preparation of the decision and that the right to lodge a complaint was not abused by the applicant. Finally, before the litigation chamber, the SPF mentioned that pre-investigation and instigation reports are not "processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system" under GDPR. However, BDPA did not tackle this issue and therefore failed to provide for area of its decision.

USE OF ELECTRONIC IDENTITY CARD (EID) AS LOYALTY CARD

Belgian Court of Cassation, judgment of 7 October 2021.

The Court of Cassation has quashed with revert to Market Court a decision of said court, ruling that a customer is entitled to file legal action to protect his right to the minimum processing of his data in order to obtain a service, even if it was not actually processed. Market court will therefore have to rule whether a merchant can use a customer's electronic identity card as a loyalty card - without giving him any other option - or not.

By a decision of September 17, 2019 (decision 06/2019), the litigation chamber of the BDPA had declared illegal - as contrary to GDPR - the practice that consisted, for a merchant, in using the electronic identity card (and thus in processing the personal data contained on the chip) of the customer as a loyalty card, without offering him any alternative. The Authority's decision was overturned by the Brussels Court of Appeal (Market Court), in a ruling dated February 19, 2020. The Court's position was that the complainant had finally not provided her identity card to the merchant, who had therefore not effectively processed her data. In a decision of 07 October 2021, Court of Cassation overturned the decision of the Market Court, ruling that the complainant was entitled to file a complaint against the merchant's practice on the basis of her right to the minimum processing of her data in order to obtain a service, even if her data was not actually processed. The Market Court will therefore have to rule on this case again.

DATA PROCESSING RELATED TO COVID 19 EPIDEMIC CRISIS

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 143/2021 of 26 November 2021.

Appeal against a provisional measure of suspension of data processing pronounced by the inspection service of the Belgian Data Protection Authority.

On 10 November 2021, the inspection service of the Belgian DPA suspended both the verification and the processing of the Covid-19 vaccination status of candidates in the recruitment process of a hospital network. The hospital network then appealed this suspension before the litigation chamber of the BDPA. In this case, the hospital network required applicants to be vaccinated. The hospital network therefore had to process the vaccination status of the applicants. Unvaccinated applicants were not recruited. This decision is interesting for two reasons. First, it confirms that the vaccination status must be considered as health data. The chamber recalls that "health data" must be interpreted broadly. Hence, this notion concerns both the current state of health and the future state of health of the data subject. In this case, an unvaccinated person is more likely to be severely affected by Covid-19. That is the reason why his or her vaccination status is reflected in his or her medical record. Secondly, the litigation chamber concludes from the above considerations that the le-

gal basis for the processing of the vaccination status must be assessed in the light of Article 9.2 of GDPR. In this case, the hospital network relied on the legislation on staff welfare to impose a mandatory vaccination in the recruitment process and to justify the processing of the vaccination status. This argument was rejected by the BDPA, which recalled that, at that time, there was no legal provision imposing compulsory vaccination. Therefore, this legislation could not serve as a legal basis for the processing of the vaccination status.

Constitutional Court, judgment 10/2022 of 20 January 2022.

The Constitutional Court refused to suspend effects of several legal texts related to use of the Covid Safe ticket (i.e. a vaccination, test and recovery pass used to condition access to events and facilities during the pandemic).

In Belgium, access to events and facilities during the pandemic is conditioned by presentation of a vaccination, test or recovery pass named "Covid Safe Ticket" (hereafter "CST"). The national framework allowing the use of the CST is composed of (1) a cooperation agreement for which both Federal authority and federated entities must give their assent and (2) legal instruments adopted by the federated entities. Under this framework, the federal authority can impose the use of CST for activities such as mass events and federated entities are allowed to extend the use of this pass to additional events and facilities through adoption of legal texts (e.g. restaurants and sport activities). Before the Constitutional Court, the claimants requested suspension of assent texts to the cooperation agreement and the decree of the Flemish authority extending use of CST to additional facilities. According to the claimants, the disputed instruments were creating a serious harm which could not be readily remedied, which is a condition to obtain suspension before the Court, among others, due to the data processing activities inherent to use of the CST. In particular, they argued that a risk for personal data security because citizens' data are processed by numerous data controllers (i.e. each organiser and manager of events and places where CST is mandatory). The Court however ruled that personal data contained in the CST are limited to identity data and validity duration of the pass. Furthermore, the claimants failed to provide concrete and precise elements to demonstrate risk of data breaches. Hence, the claimants' harm was purely of hypothetical nature and cannot justify suspension of the disputed legal texts.

Court of First Instance of Namur, order 21/20/C of 30 November 2021.

An interim action was filed against the Walloon region for the adoption of a legal framework imposing use of the Covid Safe ticket ("CST") to control access to facilities/events on the territory of Wallonia.

In this dispute, the claimants which are non-vaccinated citizens and an association for the defense of human rights filled an interim action against the legal framework of the Walloon region for the use of CST as a mean to access activities such as restaurants sport and culture. More specifically, the claimants targeted the Decree of 21 October 2021 imposing the use of CST in Wallonia and a Decree of assent to the cooperation agreement allowing the Walloon Region to impose use of CST. In the case at hand, the Court considered that Emergency (i.e. a condition for interim action) was met, among others, because use of the CST (1) was creating a risk of habituation to present a certificate of test, vaccination or recovery in order to exercise fundamental rights and (2) was violating rights to privacy and data protection. The Court also ruled that the claimants established, *prima facie*, that the Walloon region committed a fault likely to engage its liability when adopting this legal framework. Regarding the Decree of 21 October, the court considered that this text was not sufficiently clear to interfere with fundamental rights because a 38 pages FAQ was necessary to precise situations in which the CST is mandatory. Furthermore, *prima facie* necessity and proportionality of the measure were not demonstrated by the authorities. Finally, with regard to the Decree of assent, this text was adopted in violation of Article 36.4 of GDPR in absence of prior mandatory consultation of the Belgian DPA even if this requirement was recalled by the State Council. Therefore, the Court ordered the Walloon region to take all appropriate steps to put an end to this unlawful situation. The Court also imposed a penalty payment of 5000 euros per day.

Liege Court of Appeal, judgment 2021/RF/24 of 7 January 2022.

Before the Liege Court of appeal, an appeal is lodged against the above-mentioned order of the Court of first instance of Namur (order 21/20/C of 30 November 2021). The Court annulled the order because of the prima facie proportionality of the Covid Safe Ticket ("CST").

With regard to the assent Decree to the co-operation agreement, the Court of appeal confirmed that Article 36.4. of GDPR imposes a prior consultation of the DPA when legal instruments establishing personal data processing are adopted. In this case, the assent Decree was indeed enabling data processing on the territory of Wallonia. Legislative and executive authorities have therefore no margin of appreciation on the opportunity to consult the DPA especially in a context where the CST is considered by the DPA as a serious interference with right to privacy (i.e. because access to events and facilities is conditioned to divulgation of health-related data). Thus, the Court ruled that the absence of prior consultation constitutes a *prima facie* fault of the Walloon Region. Regarding the Decree imposing mandatory use of the CST in Wallonia, the Court adopted the following reasoning. First, even if FAQs couldn't be used to specify the functioning of a Decree, it was not established that the text was *prima facie* not sufficiently precise to be understood by citizens. Second, it couldn't be ruled out that the mandatory use of the CST was contrary to several fundamental rights enshrined also in the EU Charter, including rights to privacy and data protection. The Court nevertheless considered that the Decree was *prima facie* proportionate the with the objective of avoiding congestion of the healthcare system. According to the Court, in a context where the rate of COVID-19 was high, the measure was proportionate and the use of the CST was temporary and based on a legislative norm. Furthermore, CST couldn't be used in employment context and was not based solely on vaccination certificates. The lack of prior consultation of the DPA was not sufficient to overrule the proportionality of the CST. Consequently, the Order of the Court of first instance was annulled by the Court of Appeal.

ADDITIONAL LANDMARK DECISION OF THE BELGIAN DATA PROTECTION AUTHORITY

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 11/2022 of 26 November 2021.

Decision following a complaint filed with the Berlin DPA and forwarded to the Belgian DPA under the IMI system, as the data controller was established in Belgium.

This decision deals with various violations of GDPR in the context of the placement of cookies on a website. In this case, cookies were deposited by the defendant at the first connection of the data subject on a website homepage before appearance of an information banner appeared. The defendant considered that, in order to receive the information correctly, the person had to first choose the language in which she would be informed on the homepage. It also argued that the impact of the placement of this cookie on data subject's terminal equipment was reduced because it was a necessary cookie. With respect to the language argument, the BDPA rejected it insofar as the defendant was able to provide a pre-cookie banner in English, a language commonly used in the world. As for the necessary cookie argument, the Chamber decided that, regardless of whether a cookie is necessary or not, the data subject had the right to receive prior information. The litigation chamber therefore found a breach of the principle of transparency and of the principle of prior information of the data subject. The authority also found a breach of Articles 12 and 13 of GDPR, which provide for a right to transparent and comprehensible information for the data subject who must be able to determine in advance the scope and the consequences of the processing. In this case, the defendant referred to "additional information" on its website and, therefore, did not fulfill its obligation to provide information to data subjects. Furthermore, it can be deduced from the reasoning of the BDPA that the use of an "http protocol" (and not https results) for transmitting information induced a personal data transfer in "plain". Hence, this fact is likely to violate the data controller's obligation of data security. Finally, the BDPA considered that the defendant couldn't be sanctioned for the use of a cookie wall which relates to strictly necessary cookies. This type of cookie does not require the consent of the user under ePrivacy rules because they are necessary for the functioning of the website. Hence, the defendant is allowed to subordinates access to a website to their acceptance. During the proceeding, the defendant implemented measures to comply with GDPR so that the BDPA only issued a reprimand.

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 21/2022 of 26 November 2021.

Decision following nine complaints against Interactive Advertising Bureau Europe (IAB Europe).

This case concerns the compliance of the Transparency and Consent Framework (TFC) - a framework that facilitates the management of users' preferences with regard to the processing

of their data - with GDPR and the impact of the TFC on Real-Time Bidding (RTB) (see pt. 19 et seq.). In a nutshell, RTB is the basis of online advertising placement. In this system, both the supply of advertising placements and the purchase of advertising spaces are automated by means of algorithms offering targeted advertising. These algorithms process and analyse the user's personal data in order to offer advertising that matches with the data subject's profile. Given that RTB is particularly widespread today and that data processing carried out in this context are on a large scale, this decision is quite important. As the litigation chamber points out, RTB also presents risks related to profiling and automated decision-making, correlations between data, analysis or prediction of behaviour. Regarding the lawfulness of the data processing carried out in the context of the TFC, the litigation chamber considered that both the consent and the legitimate interest of the controller, as implemented in the TFC, cannot serve as a basis for the data processing carried out (pt. 429 et seq.).With respect to transparency, the BDPA considers TCF system as non-compliant with Articles 12, 13 and 14 of GDPR to the extent that information are not provided in a transparent, comprehensible and accessible manner. The purposes were also defined too generically and the interfaces did not allow them to be easily identified. Finally, the Chamber noted, among others, violations of the principles of security, integrity and confidentiality (pt. 477 and pt. 500). The Court recognised the liability of IAB Europe for the data processing carried out by participating companies within TCF (pt. 322 et seq.) and imposed a fine of 250,000 euros to IAB Europe.

FRANCE

edited by
Philippe COSSALTER, Professor for French public Law, Universität des Saarlandes (Germany)
Hicham RASSAFI-GUIBAL, Doctor in public law

LEGISLATION AND CASE LAW

Decree n. 2021-922 of 13 July 2021.

This decree amends the Defence Code so that the General Secretariat for Defence and National Security is empowered to assist the Prime Minister in cases where a foreign state or entity disseminates fraudulent information affecting national interests on the networks. The "service for vigilance and protection against foreign digital interference" is therefore created. The activity and organisation of which is regulated by this decree.

Adapting the organizational structure public administration to the digital transformation is largely carried out by meaning of soft law. This is illustrated by two government circulars on management of data and algorithms and on the use of the State's cloud. Mention should also be made of establishment of a national service for vigilance and protection against foreign digital interference

Circular n. 6264/SG, 27 April 2021, on public data policy.

The Circular aims at strengthening the capability of the State to access high value data and exploit them. For that purpose, it creates new workstations with different functions.

Circular dated April 27, 2021 essentially develops the State's new teaching on data circulation, source codes and algorithms. The circular has three interests. On the one hand, the circular intends to strengthen the digital skills of agents already in post, particularly in the senior civil service. Objectives relating to the 'management, openness, circulation and sharing of data, algorithms and source codes' will have to be integrated within assessment criteria for senior managers. In addition, circular envisages strengthening administration's relationship with actors possessing data of general interest with high added value for the public authorities' and provides for the creation of a 'mediator of data of general interest' function. Lastly, and most importantly, State administration organizational tools have been rethought to include "ministerial administrators" or "referents" at each ministerial and decentralised level. The code.etalab.gouv.fr platform should enable dissemination of public source code, based on the model of the data.gouv.fr platform.

Circular n. 6282/SG, 5 July 2021, on the doctrine for the use of cloud computing by the State.

The circular begins by setting out the regulatory framework and outlining the public authorities' approach in France from the start of the implementation of eGovernment through cloud-based e-services. It then sets out the situation up to the beginning of 2021, distinguishing between the State's internal cloud, the cloud service for public procurement and the support services put in place for the implementation of these services.

This review of the situation leads to the conclusion that the results have been positive and that it is appropriate to continue along these lines, to the point of establishing a strategy known as "cloud at the centre". One of the objectives of this strategy will be to promote a cloud culture and analyse the use of this technology by IT teams and users.

The circular of 5 July 2021 (JCP A 2021, act. 487) translates into law the political will to develop cloud hosting of the State's IT services. The circular itself is relatively short and essentially constitutes the basis for introduction of a technical document entitled Doctrine 'cloud at the centre' for using cloud computing within the State. The main objective of this act is to provide to accelerate the deployment of a 'cloud culture' within the central and decentralised administration, through the obligation to use cloud hosting for any new IT development or any 'substantial' modification of an existing tool (i.e. any modification involving a change of service provider or an evolution 'representing at least 50% of the manufacturing cost of the initial product'). In perspective opened up by circular of 8 November 2018 (n. 6049/SG), circular distinguishes three categories of cloud computing systems: 'internal' cloud, which is entirely and directly managed by State, benefiting from special protection in order to ensure continuity of State, a 'dedicated' cloud that relies on commercial offers customised for the State's needs and based on dedicated infrastructures, and a "commercial" cloud, consisting of a catalogue of solutions commonly offered by the market. Circular drafted 5 July 2021 proposes a variation on principle of continuity of public service in digital administration: continuity of public service now requires reversibility, portability, interoperability, IT security and sovereignty. The concept of 'digital sovereignty' is understood here, in a relatively restricted sense, as capacity of State and its IT systems to stay independent from non-European law, contrary to broader meaning of the term presented in the report on behalf of the Senate's committee of enquiry into digital sovereignty of 1 October 2019 (No. 7, spec. p. 103). The circular of 5 July 2021 renders applicable to State services the reference framework and technical requirements established in the framework of the GAIA-X project, an European Union-wide data infrastructure project managed by a non-profit association under Belgian law, and intended to become the project on which the European Union's data industrial strategy should be built (U. von der Leyen, State of the Union 2020 speech, 16 September 2020: https ://ec.europa.eu/info /sites/default/files/soteu_2020_en.pdf. - See also, European Economic and Social Committee, Opinion, 18 June 2021, Digital targets for 2030). The submission of the French State's cloud to harmonized technical requirements at European Union standard is likely to open up possibility of a leap in scale and the creation of State clouds in trans-European networks.

Decree n. 2021-922, 13 July 2021, creating, under the Secretary General for Defence and National Security, a national service called "Service de vigilance et de protection contre les ingérences numériques étrangères" (Vigilance and Protection Service against Foreign Digital Interference).

Institutions and administrative organization reforms on State's cloud services and digital sovereignty.

Decree 2021-922 of 13 July 2021 extends the above objective of powers held by Secretary General for Defence and National Security (Secrétariat général de la défense et de la sécurité nationale), under the direct authority of the Prime Minister, by making him responsible for "identifying operations involving, directly or indirectly a foreign state or a foreign non-state entity, and aiming at the artificial or automated, massive and deliberate dissemination, through an online public communication service, of allegations or imputations of facts that are clearly inaccurate or misleading and likely to harm the fundamental interests of the Nation".

This new competence, which is broadly worded, joins list of competences it already had in digital matters, namely that of providing the President of the Republic and the Government with the provision and operation of an electronic command and communications network in defence matters (Code de la défense, art. R. 1132-3, 6°) and that of proposing to the Prime Minister (whose competence is established in C. défense, art. L. 2321-1) and implementing the Government's policy on the security of information systems (C. défense, art. R. 1132-3, 7°).

Secondly, and in order to provide Secretary General for Defence and National Security with the means to exercise his new powers, Decree 2021-922 creates the national service of vigilance and protection against digital interference (Service de vigilance et de protection contre les ingérences numériques étrangères). This service is responsible for 'detecting and qualifying' all massive online disinformations, provided that they are, among other things, 'of a nature to un-

dermine the fundamental interests of the Nation', and in particular, according to Article 3 of the aforementioned decree, those referred to in Article 33-1-1 of Law 86-1067 of 30 September 1986 on audiovisual communication, i.e., those initiated by an entity "controlled [...] by a foreign State or placed under the influence of that State" and whose purpose is to disseminate "in a deliberate manner, false information likely to alter the sincerity of the vote".

As for the means at the disposal of this service, the decree remains silent. In particular, no one knows the categories from which the civil servants will be recruited or the skills that the public servants assigned to it will have to have. The operational and legal resources available to the service are also unknown. Although it will be responsible for detecting disinformation operations "by analysing publicly accessible content on online platforms", the truth remains that the authorised data processing is not (yet) known. It should also be noted that the fact that the content is publicly accessible does not make data processing immune from need to respect right to privacy (see *mutadis mutandis*, concerning the experimentation authorised for benefit of tax authorities by Article 154 of the Finance Act for 2020: Conseil constitutionnel, 27 December 2019, n. 2019-796 DC. - And CNIL, deliberation n. 2020-124, 10 december 2020, and review below). Finally, Decree n. 2021-922 does not grant the Service de vigilance et de protection contre les ingérences numériques étrangères or the Secretary General for Defence and National Security any powers of sanction, constraint or coercion. While it is understandable that the aim of this service is to enable an early reaction to disinformation campaigns, and thus to counter effects of Brandolini's law (according to which the energy needed to counter false information is of a greater order of magnitude than that needed to disseminate it), one may wonder about the real effectiveness of such a service. Apart from its already planned mission of 'assisting' the Secretary General, or that of 'providing any useful information' to the Conseil supérieur de l'audiovisuel (CSA) and the National Commission for the Control of the Electoral Campaign for the Presidency of the Republic (provided for in Article 13 of the D. 2001-213), this new service is in serious danger of being confined to role of digital watchdog, or even producer of 'fact checking' content.

ADMINISTRATIVE ACTS

Council of State, united chambers, 5 May 2021, n. 434007, Sté DMP Corporation.

The General Meeting of the Superior Council of Notaries, through a public tender procedure, intended to subcontract notarial activities with third parties, establishing certain confidentiality requirements and the adoption of ethical codes, as well as the need to have the corresponding ETIC labeling. This decision is appealed by a company, and in resolution nº 434007 of May 5, 2021, of the Conseil d'Etat decides on this possibility, concluding in this regard that the Superior Council of Notaries does not have legislative competence to authorize the subcontracting of certain notarial activities, nor to impose a labeling procedure for subcontractors who manipulate electronic data of notaries, despite the obligation of these to electronically manage the data they use.

Dematerialization of notarial activities requires mandatory use of IT solutions offering guarantees of security, integrity and confidentiality. The Conseil national du notariat, an authority of public utility was entitled by Article 16 of Decree No. 71-941 of 26 November 1971 on deeds drawn up by notaries with approving the system or systems for processing and transmitting notarial information. On this basis Conseil supérieur du notariat adopted a resolution on 2 and 3 July 2019 establishing 'as a first step', pending possible regulation 'at a later stage', the rules applicable to notaries' subcontractors. The Conseil d'Etat rescinds the resolution on the ground of lack of jurisdiction (JCP N 2021, act. 659).

The Conseil d'Etat grounded its decision on 3 points: 1. the labelling is not provided for by any legislative or regulatory text; 2. the resolution anticipates an approval procedure that does not exist and defines its scope, whereas no legislative or regulatory provision assigns this competence to the Conseil supérieur du notariat; and 3. the resolution prohibits subcontracting of certain acts whereas no legislative or regulatory text provides for such a prohibition.

This decision of the Conseil d'Etat raises two points. On the one hand, certain texts that initiate a dematerialisation process often turn out to be imprecise or incomplete. On the other hand, this relative 'vacuum' is filled by practitioners who, in so doing, exceed their own competence.

Article 11 of Law n. 2016-1321 of 7 October 2016 for a Digital Republic created article L. 321-3 of the Code on relations between the public and the administration (CRPA).

The introduction by this rule of article L-321-3 in Law 2016-1321 implies that, without prejudice to the intellectual property rights of third parties, Public Administrations may not prevent the reuse of the content of the databases that they publish and make available to third parties, except those that have been produced by the Public Administrations as part of the provision of a public service that has an industrial character or commercial.

While fact of the given product data produced in the context of direct management is (in principle) easy to forsee, relationship with the Administration's co-contractors in event of recourse to public contracts or concessions is more complex. The property of the data produced may be questioned and, above all, although the obligation to disseminate is incumbent on the administrations, it does not seem to be imposed directly on co-contractors and must find expression in the contract.

FNCCR model contract.

National Federation of awarding authorities (concession) (*FNCCR*) has already introduced a stipulation on the re-use of the data produced into its model contract for electricity distribution published at the end of 2018. According to Art. 15 of the *FNCCR* model contract, distribution system operator shall communicate to concessioning authority and to competent local authorities or public establishments data from metering devices that are useful exercising of their competences, in particular those that make it possible to draw up and evaluate the regional climate, air and energy plans and the territorial climate-air-energy plans provided for in Articles L. 222-1 to L. 222-3, L. 229-25 and L. 229-26 of the Environmental Code.

Article 16 B then provides for the transmission to the public of data relating to the capacity of networks upstream of source substations and the capacity of these substations, for competitive reasons.

This contract model that can be adapted with difficulty in practice must be referred to a specific subject.

The new CCAG.

Effects of new provisions introduced in the model General Administrative Conditions of Contract (Cahiers des clauses administratives générales - CCAG) for public procurement may be much wider. Six CCAG were published on 1st April 2021. They all contain, in articles that may differ slightly, which makes it impossible to cite them in a coordinated manner, three types of stipulations relating to the data produced. Firstly, the co-contractors are subject to the RGPD and must therefore ensure the protection of the personal data collected (CCAG, art. 5). Secondly, the CCAG (with the exception of the works CCAG) deal with the fate of data essential to the performance of a public service. Thirdly, the GCC deal very comprehensively with the re-use of "results". The results "refer to all elements, whatever their form, nature and medium, which are produced in the context of the services of the contract, such as, in particular, intellectual works (including software and their documentation), databases, [...]" (CCAG Intellectual services (*Prestations intellectuelles*), Art. 32.1). The CCAG PI provides, for instance, for the results consisting of databases to be extracted and used freely by the purchaser "in particular with a view to making public information available for re-use free of charge or against payment" (CCAG PI, Art. 35.4.3).

PUBLIC SERVICES

D. n. 2021-279, 13 March 2021, containing various provisions relating to the national identity card and the processing of personal data known as "secure electronic documents" (TES).

The decree implements the provisions of the Regulation EU 2019/1157 of the 20 June 2019 on strengthening the security of EU citizens' identity cards and the residence documents issued to EU citizens and their family members exercising their right to free movement. Firstly, the decree states that, within the national identity card, an electronic component comprising biometric elements, digitized image of its holder and two fingerprints, must be integrated. It also imposes mandatory collection of fingerprints, except for minors of 12 years, reduces the period of validity of national identity cards to 10 years, and requires the presence of an electronic stamp visible on the title containing signed data of the holder. In addition, the decree makes changes to the procedure for issuing identity cards concerning people who are detained or physically unable to move. For these subjects, photographs are taken by prefecture or town hall officials who travel with a mobile device to record the applications for identity cards.

Introducing electronic national identity card

(CNIe), rendered mandatory by Regulation 2019/1157 of 20 June 2019, applicable since 2 August 2021, required adoption of Decree No. 2021-279 of 13 March 2021 containing various provisions relating to national ID card and processing of personal data known as 'secure electronic documents' (TES) and led the CNIL to issue its opinion No. 2021-022 of 11 February 2021.

Decree n. 2021-279 of 13 March 2021 adapts Decree No. 55-1397 of 22 October 1955 to the new security requirements for national identity cards.

In order to reduce cases of identity theft, the decree states that, within the national identity card, an electronic component comprising biometric elements, digitized image of its holder and two fingerprints, must be integrated. It also imposes mandatory collection of fingerprints, except for minors of 12 years, reduces the period of validity of national identity cards to 10 years, and requires the presence of an electronic stamp visible on the title containing signed data of the holder.

This adaptation aims to improve the security of identity documents and, consequently, to strengthen the fight against identity theft, which the ministry indicates affects 200,000 people per year. The CNIe will now have several secure electronic components, including an "electronic component", i.e. an electronic chip engraved with a Marianne and an electronic stamp as provided for in Regulation 910/2014 of 23 July 2014 known as eIDAS (but whose level of certification - simple, advanced or qualified - is unknown).

National digital identity card: CNIL, Deliberation n. 2021-022, 11 February 2021, on a draft decree amending Decree n. 55-1397 of 22 October 1955 establishing the national identity card and Decree n. 2016-1460 of 28 October 2016 authorising the creation of a personal data processing system relating to passports and national identity cards (request for opinion n. 20015262).

Giving its opinion on the draft decree, the CNIL highlights the sensitivity of the data contained in the TES file and recalles that, according to Cons. const., 22 March 2012, n. 2012-652 DC, the use of these data should be limited only for the purpose to which they were acquired, in order to better protect the privacy needs of citizens. Although these reversations, the CNIL states that the CNIe will be an important milestone on the road to establish a real "State digital identity" and an opportunity to access to a secure device offering digital identity services. In order to maximise the benefits of instrument, the Commission stresses the importance of taking into account the issues related to digital inclusion, especially for people with disabilities.

On 11 February 2021, CNIL issued its opinion on the draft decree, which became decree no. 2021-279 of 13 March 2021, refered to above. The CNIL's opinion is interesting in several respects. First of all, it should be remembered that the implementation of the CNIe will require access to the TES file, which contains the civil and physical identification details of people holding a national ID card or passport. However, drafting of this file, initially provided for by the law of 27 March 2012 on the protection of identity, was censured by Constitutional Council (Cons. const., 22 March 2012, No. 2012-652 DC). Sensitivity of a file containing the identity data of all (or almost all) nationals, which detractors had renamed the "database of honest people", meaning that the use of data should be limited to the sole purpose of issuing and checking validity of identity documents, to the exclusion of any administrative or judicial police purpose. In addition, risks associated to creation of such a sensitive centralised database had led the CNIL to express serious reservations about the creation and use of this file (CNIL, deliberation no. 2016-292, 29 September 2016). The TES file, finally created by Decree No. 2016-1460 of 28 October 2016, now contains the surname and first names, date and place of birth, sex, eye colour, but also the digitalized image of the face, fingerprints, or even email address and telephone number, if applicable, of the citizens concerned. In its opinion of 11 February 2021, CNIL reiterated its reservations about such a file, pointing out that it remains a 'singular file' so that it has always been particularly attentive to substantial guarantees to be implemented in order to supervise use of this processing and intends to exert control in the context of the changes taking place

Having set out reservations of principle, it should be mentioned that the CNIe is an important milestone on the road to establishing a State digital identity that should make it possible both to identify a person (to know the identity of a person) and to authenticate him or her (to verify that the person concerned is who he or she claims to be). The CNIe's electronic components will therefore be integrated into existing authentication solutions, such as ALICEM (see below) and FranceConnect. With this objective of mak-

ing the CNIe the central element of a State digital identity system, CNIL also recommends considering possibility that the electronic components may deliver only part of the information contained, thus aiming to minimise and adapt the information delivered to the various services (public and private) according to the needs of the service in question. The institution of a 'State digital identity' constitutes a pre-emption by the State of the role of online trusted third party in the (regalian) domain of civil status and constitutes an interesting example of State digital extension.

Finally, it should be mentioned that the CNIL, like the Defender of Rights (*Défenseur des droits*); see in particular its decision No. 2020-027, 20 May 2020), remains particularly attentive to the accessibility of public services, especially for people with disabilities. One might add to the above that digital disability, more generally, may also constitute an additional difficulty, which it would be regrettable to underestimate (see also, Défenseur des droits, *Dématérialisation et inégalités d'accès aux services publics*: report 2019).

ADMINISTRATIVE POLICE

Decree n. 2021-464, 16 April 2021, extending the scope of information and data exchanges between administrations in the context of administrative procedures - Draft law on differentiation, decentralisation, deconcentration and various measures to simplify local public action (known as '4D').

The amendments made by the decree of 16 April 2021 extend the scope of exchanges of information or data between administrations by adding the mandatory census of citizens. This amendment completes the list of information and data exchanged between administrations and designates the administrations from which the communication of this information or data is requested. Thus, information on people's income, diplomas, titles and professional qualifications will be the subject of these exchanges, as well as information on the situation of the family, schoolchildren, jobseekers and persons with regard to the obligations laid down in Article L. 111-2 of the National Services Code.

The principle established by the Law for a Digital Republic in Article L. 114-8 of the Code of Relations between the Public and the Administration aims to reduce formalities to be finalized by citizens in their exchanges with Administrations. It provides for administrations to exchange with each other all the information or data (strictly) necessary to process a request or a declaration from a citizen.

Decree n. 2021-464 of 16 April 2021 substantially amended the scope of information which, pursuant to Article R. 1114-9-3 of the CRPA, may be exchanged between administrations, by including income, diplomas, educational situation of pupils, the situation of job seekers, the family situation and the military situation of citizens. Is extended the area of justification and legitimacy for the exchange of information.

This extension of the exchange of information between administrations does not stop there. The so-called '4D' bill, which is currently examined by the National Assembly, envisages amending, in particular, Articles L. 114-8 and L. 114-9 of the CRPA in order to remove the list of areas concerned by possibility of exchanging information between administrations. Data exchange becomes the standard. In addition, the bill provides that administrations will henceforth be able to spontaneously request information from other administrations, without any prior request or declaration from citizens concerned, for the sole purpose of informing them of their right to a possible benefit or advantage. Finally, it intends to increase transparency by establishing a public list of the categories of data exchanged. It should be noted, however, that at first reading, the Senate sought to exempt municipalities with fewer than 10 000 inhabitants from obligation to exchange information, thereby substantially restricting the scope of the administrations concerned.

The exchange of information between administrations has a definite positive effect on the functioning of administrative action. It makes it possible to combine the advantages, in terms of security, of decentralised databases, and we know that the CNIL is reluctant to allow the creation of databases that are too large (see, for example, the "TES" file), with power of networking the information held by the various administrations. The networking of administrative databases and the cross-referencing of the data they contain should enable the State, in particular, and public bodies, in general, to (re)create profiles or digital "avatars" of citizens, which is not without raising some fundamental questions in the long term (see, for example, the report on the "TES" file, on page 10, A. Rouvroy and B. Stiegler, *Le régime de vérité numérique. De la gouvernementalité algorithmique à un nouvel État de droit*:, in *La nouvelle revue des sciences sociales*, 2015, n. 4, 113-140).

Platform and public service: Council of State, ord., 13 March 2021, n. 450163, Assoc. InterHop et a.

It is not necessary to request an opinion from the National Commission for Informatics and Liberties to ascertain that the decision of the Minister for Solidarity and Health to entrust a private company with the management of vaccination appointments against Covid-19, in order to ensure their rapidity, does not constitute a serious and manifestly unlawful infringement of the right to privacy and the protection of personal data, also in view of the data protection arrangements ensured by that company

In this decision of 13 March 2021, the Conseil d'Etat rejects the petition presented by professional associations against "partnership" by which Minister of Health and Solidarity entrusted Doctolib platform, among other things, within management of booking of vaccination appointments, in the context of the Covid-19 pandemic. Beyond the legal point on the hosting of data by AWS, a subsidiary of an American company, but nevertheless holder of the health data hosting certification provided for in Article L. 1111-8 of the Public Health Code, the order is of interest insofar as it shows that the State did not have ability to develop an online appointment scheduling system in a timely manner. Moreover, one wonders about the exact legal nature of this "partnership" and the possible compensations from which Doctolib benefited.

Decree n. 2021-1048, 4 August 2021

This measure aims to develop a digital health space through an app based on two specific pillars. It would be possible to find in that web the shared medical file and also a wide range of services available for the users and offered by public authorities and private operators.

Decree n. 2021-1048 of 4 August 2021 specifies the legal framework for the deployment of the digital health space, provided for in Article L. 1111-13 of the Public Health Code, resulting from Law No. 2019-774 of 24 July 2019 on the organisation and transformation of the health system.

In any case, the decree does not specify or mentions that, the digital health space will be accessible by a mobile phone app

The digital health space has two important features. Firstly, it is a solution that aims to bring to life the shared medical file (Dossier médical partagé, DMP), which has been in the making since the law of 13 August 2004 and which the Cour des comptes (Court of Auditors) was already highlighting in 2013 the considerable expenses incurred for a disappointing result (Cour des comptes, Le coût du dossier médical personnel depuis sa mise en place, Communication to the National Assembly's Finance Committee, July 2012, published on 13 February 2013). Secondly, although it is a space developed and hosted by the State, a catalogue of services will be accessible to the user and will offer modules developed and proposed by private companies. The hypothesis of a specific regime for the "occupation of the State's digital public domain" should provide food for thought in the future.

Urban video surveillance: CNIL, Warning to the City of Valenciennes, 12 May 2021.

The situation under analysis occurs when the company Huawei donates to the city of Valenciennes devices worth €2 million to implement a "smart" video surveillance system, in exchange for a maintenance contract of €34,000 over 3 years. The authorities are concerned because through these devices the company has access to all the facts and information that occur in the city.

Video surveillance field is an area of developing legal problems, particularly with regard to "smart cities". The online news website Mediapart revealed the existence of a warning letter sent by the CNIL to the city of Valenciennes (1 August 2021, Videosurveillance: Valenciennes and its "safe city" model outside the law: www.mediapart.fr/journal/france/010821/videos urveillance-valenciennes-et-son-modele-de-safe-city-hors-la-loi) concerning the deployment of a "smart" video surveillance system. The particularity of this affair, which to the authors' knowledge has not been followed up, lies in the fact that the company Huawei (which the United States considers a threat to its internal security - Les Echos, Huawei reste dans le collimateur des Etats-Unis, 13 March 2021: www.lesechos.fr/ tech-medias/hightech/huawei-a-nouveau-dans-le -collimateur-des-etats-unis-1297991) offered the city of Valenciennes equipment worth more than €2 million, in exchange for a maintenance contract of €34,000 over 3 years. Many questions have been raised about this generous "gift" from a private company to a municipality, especially since the CNIL revealed that the video surveillance system was used for automatic reading of licence plates, and could also be used to detect the removal or deposit of an object, as well as intrusion into or exit from an area, rapid move-

ments, lingering in an area, counting people, assessing crowd density, movements with abnormal speed, alerting to the detection of a particular plate, and route detection. Could the 'donation' to the city have been used to train the algorithms developed by Huawei in real life?

Furthermore, a journalist from the information website L'observateur du Valenciennois indicated that she had been remotely fined for not wearing mandatory mask, even though she had not come across any police officers (*L'observateur du Valenciennois, Valenciennes rappelée à l'ordre : la vidéoprotection y est jugée particulièrement intrusive*, 3 August 2021: www.lobservateur.fr/valenciennois/valenciennes/2021/08/03/valenciennes-rappelee-a-lordre-la-videoprotection-y-est-jugee-particulierement-intrusive/). Would Valenciennes have had the same desire to innovate as the Paris police prefecture, by setting up a 'wild' facial recognition system? The question has been raised. We are now waiting for the outcome of the legal proceedings to hopefully have at least the beginning of an answer.

Council of State, ord, 6 July 2021, n. 453505, Assoc. La Quadrature du Net.

In a judgment of 6 July 2021, the Conseil d'Etat rules on the technical and legal reasons which may lead to the choice of a decentralised information storage system. In particular, the different advantages and disadvantages of adopting a centralised or decentralised database solution.

In a judgment of 6 July 2021, the Conseil d'Etat rejected the application for interim relief lodged by the association "La Quadrature du Net" against the "Health pass" system. The applicant association argued that the inclusion in the two-dimensional code (QR code) of information concerning the civil status or health status of citizens broke the right to privacy and the right to respect for the protection of personal data. The order is of interest insofar as the interim relief judge of the Conseil d'État details, in his reasoning, the technical and legal reasons that led to the choice of a decentralised system for storing information. This reasoning thus presents a possible trade-off between a centralised database solution, on the one hand, and a solution that relies on decentralised databases operating without any (or only very limited) exchange of information, on the other, a trade-off that could give rise to reflection in other areas.

REGULATION AND PUBLIC COMPETITION LAW

Communication system for fire, rescue and civil protection services D. n. 2021-970, 21 July 2021 "NexSIS 18-112".

This document incorporates the provisions of the Homeland Security Code regulatory part (new articles D. 732-11-19 to D. 732-11-23) by establishing a unified information and command system for fire and emergency and civil security services, called "NexSIS 18-112". This system is aimed to offer the population a high-quality service, in particular for processing alerts received through emergency numbers and the operational management of emergency resources. The text establishes that the digital civil security agency will carry out the studies, design, development, deployment and provision of the unified information and command system "NexSIS 18-112". It provides that the "NexSIS 18-112" system will ensure: the processing of alerts received via the emergency numbers 18 and 112; communications between the population and the emergency services; operational and crisis management provided by the fire and rescue and civil security services; interoperability with the information systems of public and private entities contributing to civil security. It defines the confidentiality, data protection and security requirements that the system must satisfy.

The movement to centralise computer networks supporting public service missions for reasons of efficiency and interoperability is also expressed in the general area of civil protection. Decree 2021-970 aims to implement a single IT system called NexSIS 18-112 for all fire and rescue services and civil protection services. This system is implemented by the Civil Security Digital Agency, created by Decree No. 2018-856 of 8 October 2018.In application of its case law Ordre des avocats au Barreau de Paris (CE, ass, 31 May 2006, No. 275531), the Conseil d'État (CE, 14 Oct. 2020, n. 426119, Assoc. Qualisis et a.) rejected the appeal on the grounds that (1) the agency thus created met the need to satisfy a general interest requirement, namely to improve the efficiency of the system for transmitting information between the various services concerned and to reduce its costs, and (2) Decree No. 2018-856 was not in itself such as to lead the agency to distort the free play of competition on the market. On the other hand, in a decision of the same day (CE, 14 Oct. 2020, No. 428691, Assoc. Qualisis et al.), the Conseil d'État rescinded Decree No. 2019-19, granting to the civil security digital agency the exclusive right to supply fire and rescue services or civil security

services with all or part of the systems, applications or services falling within the scope of the unified command and information system NexSIS 18-112. For reasons of economy of means, the Conseil d'Etat had only annulled the decree on the grounds that it violated Article L. 462-2 of the French Commercial Code, which requires the Competition Authority to issue a prior opinion on any draft text instituting exclusive rights.

The Government finally complied with this obligation (ADLC, 30 Apr. 2021, n. 21-A-06). Decree No. 2021-970 of 21 July 2021 reproduces almost identically the provisions of Decree No. 2018-856, which was voided by the court, with two exceptions: on the one hand, exclusive right is now limited to 10 years, renewable for a period of five years, whereas previously it had no time limit, and on the other hand, it seems that the Prime Minister has finally given up on the idea of doubling the exclusive right by requiring SDISs to use the NexSIS 18-112 service (V. not. ADLC, 30 Apr. 2021, op. cit, p. 14-16). In so doing, one wonders about the interest of implementing a centralised system, which is supposed to guarantee the efficiency and interoperability of local systems, objectives that constitute the justification for establishing a service of general economic interest, while its deployment is not generalized but is left to the discretion of individual administrations.

Administrative Court of Appeal (CAA) Lyon, 1 oct. 2020, n. 19LY00254, Sté R et L.

The Lyon Administrative Court of Appeal stated that an employment contract between the UBER company and the drivers did not qualify as an employment contract, as the drivers were not linked to the company in terms of subordination. For this reason, the Prefect's decision ordering the closure of the establishment that operated the platform was annulled, as the relationship between the latter and the drivers was qualified as undeclared work.

The "platformisation" of the economy (Conseil d'Etat, *Puissance publique et plateformes numériques : accompagner l'ubérisation*, Annual study 2017) affects more and more fields, and calls for an increasingly extensive control by the Administration. It is in this context that the Administrative Court of Appeal (CAA) of Lyon addressed a case concerning a platform for putting driving licence candidates in contact with self-employed driving instructors. After an investigation by competent Directorate, the Administrative authority (*Préfet*) ordered administrative closure as a sanction of establishment operating platform, having qualified the relationship between the platform and the instructors as undeclared work. The legal debate concerned whether the contractual relationship between the platform and the instructors should be qualified as an employment contract, because of the decision of the Cour de Cassation which qualified the relationship between the Uber company and a driver as an employment contract (Cass. soc., 4 March 2020, n. 19-13316). After examining the conditions under which rates for services offered by the instructors are defined, terms of exercise of these teaching services, the evaluation by the candidate-clients, and the existing sanctions, the CAA of Lyon concluded that there was no link of subordination and cancelled administrative sanction. The "*uberisation*" of the economy is far from being just a memory.

Council of State, ord., 4 March 2021, n. 449212, Google LLC et Google Ireland.

France's highest administrative court (Conseil d'Etat) rejected a request for interim measures filed by Google LLC and Google Ireland Limited. The request concerned the removal, within three months, of a sanction imposed by the CNIL on Google to comply with the regulation on the principle of data processing, with a penalty of €100,000 per day of delay. The court stated that Article 82 of the Informatique et Libertés law was a transposition of Article 5(3) of Directive 2002/58/EC into French cookie law and that the CNIL is in charge of enforcing this directive. As such, the one-stop shop mechanism provided for in Article 56 of the GDPR does not apply to the present case.

It is worth mentioning this interesting order of the *interim* suspension judge of the Conseil d'Etat, in appeal lodged by Google LLC and Google Ireland against an injunction to comply issued by the CNIL concerning the use of computer cookies when using the search engine Google Search. The interest of this order could be anecdotal except that one could have thought that it was likely to weaken the mechanism of the "lead" or "one-stop shop" authority set up by Article 56 of the RGPD, which we know organises the cooperation of national supervisory authorities when a processing of personal data is cross-border. Indeed, the applicant companies argued that the French CNIL was not territorially competent to adopt the contested injunction. The Conseil d'Etat rejected the request on the grounds that the legal regime applicable to cookies was based, in this case, on Directive 2002/58

of 12 July 2008, known as the "Privacy and Electronic Communications Directive", and not on the RGPD, which does not provide for a "one-stop shop" mechanism. In this way, Conseil d'Etat anticipated an important ruling of the CJEU with a convergent solution (CJEU, 15 June 2021, case C-645/19, Facebook Ireland et al. v. Gegevensbeschermingsautoriteit).

PUBLIC FINANCE

Decree n. 2021-148, 11 February 2021, concerning the implementation by the Directorate General of Public Finance and the Directorate General of Customs and Indirect Rights of computerised and automated processing allowing the collection and exploitation of data made public on the websites of online platform operators.

Sandbox regulation will allow, for the next 3 years, the tax and customs administrations to collect and exploit content freely accessible and obviously made public by users on the websites of online platform operators for the purpose of investigating certain offences.

While the Directorate General of Public Finances (Direction générale des finances publiques – DGFIP) annual report for 2020 states that data mining has enabled the recall of 794 million euros in duties and penalties (DGFIP, Annual Report 2020, p. 13) and that 32% of controls are targeted by artificial intelligence (Ibid., p. 30), automated data processing by tax administrations is undergoing a major new development. Article 154 of Law No. 2019-1479 of 28 December 2019 on finance for 2020 authorised, on an experimental basis for a period of 3 years, the tax and customs administrations to collect and exploit content freely accessible and obviously made public by users on the websites of online platform operators for the purpose of investigating certain offences. It should first be recalled that the Constitutional Council censured certain parts of this provision, thus reducing the scope of the offences included in the experiment (Cons. const., 27 Dec. 2019, No. 2019-796, Finance Act for 2019). Decree No. 2021-148 of 11 February 2021 specifies the terms and conditions for processing (collection, development and use) of the data collected.

Only "content freely accessible and obviously made public" and "access to which does not require the entry of a password or registration on the site in question" may be processed. Tax and customs authorities will also not be allowed to use accounts with an assumed name or specialised accounts for data collection, except for those necessary for the use of the API (automatic programming interface) of the platform or social network in question, and allowing the automation of data collection.

Basically, from the creation of profile-types to be developed by administrations concerned during the learning and design phase of the algorithm, it will be possible (1) to associate an account on a platform or a social network with a particular citizen and (2) to relate the data made publicly accessible by the citizens on the platforms and social networks, and (3) to identify possible offences specifically targeted (smuggling, unauthorised import or export, including of tobacco, fraud concerning tax domicile, hidden activities, fraudulent manufacture of alcohol, etc.).). To this end, a decree of 8 March 2021 allows the data thus collected and the processing algorithm to be linked to the CFVR ("targeting fraud and enhancing requests") processing system, which is a flagship project for the digital transformation of the tax administration (see www.bercynumerique.finances.gouv.fr/vivre-le-numerique-a-bercy/le-data-mining-a-la-dgfip).

In this context, the recurrent debates on online anonymity (or more precisely pseudonymity), generally initiated in the context of the fight against offences committed against persons, find a particular echo in the context of tax audits. Since administrative authorities can only rely on publicly available information on social platforms and networks, a possible ban on pseudonymity could be of definite (collateral) benefit to tax and customs authorities heritage.

It should also be noted that, for the first time, tax and customs authorities will be able to feed their data by "dipping" directly into the incredible mass of information provided by the concerned people themselves on social networks, in particular. This once again proves Bernard E. Harcourt, the American translator of Michel Foucault, right. In his book Exposed (*Desire and Disobedience in the Digital Age*, Cambridge-London, Harvard University Press, 2015) anticipates a fundamental shift in the way state surveillance works: whereas state used to have to intrude into private lives of its citizens in order to collect information, it can now simply help itself to data 'exposed' by the citizens themselves.

GERMANY

edited by
Marius HUNDT, Research fellow at the Chair of International Law, European

Law and Comparative Public Law at the University of Leipzig.

NECESSARY INFORMATION ON THE POSSIBILITY TO FILE FOR LEGAL REMEDIES ELECTRONICALLY

Federal Administrative Court, judgment 9 C 8/19 of 25 January 2021.

In this case, Federal Administrative Court had to deal, among other things, with the question of whether electronic transmission is an independent form of filing an action.

The plaintiff, who is resident in the United States, received a notice of costs from a German authority in January in which he was to share in the costs for the extension of an adjacent road to his property in Germany. With the same notice, he was informed that he could bring an action before the administrative court in Göttingen, Germany, within one month "in writing or for recording (*schriftlich oder zur Niederschrift*)". The one-month period is derived from section 74 (1) of the Administrative Court Procedure Act (*Verwaltungsgerichtsordnung – VwGO*). His registered letter by post was received by the Administrative Court only after a considerable delay, so that the one-month deadline was not met. The applicant then applied for *restitutio in integrum* (*Wiedereinsetzung in den vorigen Stand*). He argued, inter alia, that the notice of appeal of the authority's decision was deficient. The possibility of electronic data transmission should have been expressly stated in notice, as this is not just a special form of written transmission of a complaint, but an independent form of filing a complaint. In this case, the Federal Administrative Court ruled that the authority's action was not objectionable. The possibility of filing an appeal by electronic means is expressly mentioned in the Administrative Court Procedure Act (more precisely in § 55a (1)) and is included in the wording of "filing an action in writing" (in § 81 (1) sentence 1 of the Administrative Court Procedure Act). The Federal Administrative Court shares the view of the lower courts that the transmission of the statement of claim as an electronic document is not a separate form of bringing an action, but a written statement of claim. The action was ultimately dismissed as inadmissible.

Higher Administrative Court of Schleswig-Holstein, decision 2 LB 15/19 of 15 June 2021.

In a case similar to the above-mentioned, the Higher Administrative Court of Schleswig-Holstein decided otherwise.

Again, the issue was the wording "in writing or for recording" in the information note on legal remedies (*Rechtsbehelfsbelehrung*). Again, the plaintiff argued that this did not include the electronic form of filing an action and that the instruction was therefore insufficient. In this case, the Higher Administrative Court of Schleswig-Holstein agreed with the plaintiff's argumentation. The possibility of filing an action electronically was not a sub-case of filing an action in writing but rather an independent possibility. The wording "in writing or for recording" in the information note on legal remedies was therefore objectively capable of causing the recipient to make a mistake. Therefore, the instruction on legal remedies was defective. The Higher Administrative Court upheld the action.

Higher Regional Court of Hamm, judgment 4 U 1/20 of 10 June 2021.

In this case, the Higher Regional Court of Hamm determined that, in order to grant effective legal protection, reference may exceptionally be made to data from a digital storage medium (e. g. a USB-Drive).

The plaintiff in this case operates, among different magazines and newspapers, an online news portal. The defendant city administration also operates a website on which, in addition to official notices, special news from the surrounding area was also posted in the form of its own news portal. According to the plaintiff, the city thus presents itself as a local daily newspaper and thus exceeds the permissible scope of municipal public relations. In doing so, the plaintiff largely relied on content from a USB storage medium. In this regard, the Higher District Court stated that such a reference to digitally stored content may be permissible by way of exception if effective legal protection would otherwise be jeopardised. That is the case here, as it would otherwise result in unreasonable expense for the plaintiff. In addition, a printout of the stored contents would not be able to reproduce them with the same meaning, as they are purely digital contents. There is no other possibility for a sufficiently concrete representation than through digital storage media. According to the Court, this was therefore permissible by way of exception. However, action was ultimately dismissed on the merits.

Higher Administrative Court of North

Rhine-Westphalia, decision 16 E 579/21 of 3 August 2021.

In this case, the Higher Administrative Court commented on the requirements for electronically filed documents.

The plaintiff had filed an appeal against the denial of legal aid electronically. The Higher Administrative Court ruled here that documents had already not been submitted in accordance with the Administrative Court Procedure Act. For private persons, only the sender-confirmed DE-Mail mailbox remains as a secure electronic transmission channel. The DE-Mail procedure was introduced in Germany in order to guarantee secure transmission by e-mail. Certain security mechanisms (including encryption and authentication procedures) are used. Submission via a DE-Mail mailbox is included in the Administrative Court Procedure Act as a permissible method of electronic document transmission. However, the other means of transmission listed in Section 55a (4) are not available to private individuals. Furthermore, Higher Administrative Court ruled that it is not sufficient to attach a "qualified certificate" to electronically transmitted documents. A complete electronic signature is required, of which the qualified certificate is only a part. The appeal was dismissed by the court as inadmissible.

ONLINE POSSIBILITIES FOR UNIVERSITIES

Administrative Court Gießen, decision 9 L 491/21.GI of 05 March 2021.

The court had to address whether there was a right to conduct online exams under pandemic conditions.

The applicant was a first-semester medical student and, in the present case, wanted to take the examinations due in February 2021 as online examinations. Among other reasons, he stated that he had a very long journey of more than 3 hours to the University. In addition, he was permanently taking care of two sick family members and a small child. Due to the pandemic, he was unable to place them in care and travel to the university for the exam. The university replied that it generally planned to use a combination of digital teaching and in-classroom examinations and therefore refused the applicant's request. The applicant then applied to the Administrative Court for interim legal protection. The court ultimately rejected the student's request. In its reasoning, the court stated that the university had a wide margin of discretion in selecting right form of examination. Moreover, a claim for students to conduct online examinations is not justified solely by a long journey. The Corona pandemic does not fundamentally change this.

Higher Administrative Court of North Rhine-Westphalia, decision 14 B 278/21.NE of 04 March 2021.

Here, the Higher Administrative Court had to deal with the question of whether the monitoring of online examinations by means of video and audio recordings is compatible with higher-ranking law.

Within the scope of its regulatory powers, the University of Hagen had stipulated that an examination taken by students at home was to be monitored audio-visually. In the event of irregularities or the discovery of an attempt to cheat, the corresponding video and audio recordings could also be stored for longer periods of time for the purpose of preserving evidence. The applicant took action against this within the framework of interim legal protection. He argued that it was sufficient to merely monitor the examination by means of a video and audio link. A storage of the material was not justified, since such a storage or recording does not take place also with presence examinations. However, the Higher Administrative Court rejected the application. In doing so, it first focused on the differences between online examinations and in-classroom examinations. The situations were not comparable, since the supervisor had the entire room in view during in-classroom examinations. With video supervision, only a small section of the image could be seen, which made supervision more difficult. In addition, investigations cannot be carried out immediately in order to follow up a suspicion. Finally, there was also a lack of witnesses, which made a recording necessary for later evidence. The court acknowledged that the case involved the processing of personal data and that the GDPR (General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and of the Council) therefore applied. However, this processing of data was lawful in the summary examination pursuant to Article 6(1)(e) of the GDPR, since safeguarding equal opportunities in university examinations was in the public interest. The applicant's right to informational self-determination (*Recht auf informationelle Selbstbestimmung*) therefore had to take a back seat in the balancing exercise.

Higher Administrative Court of Schles-

wig-Holstein, decision 3 MR 7/21 of 03 March 2021.

Only one day before the previous decision, the Higher Administrative Court of Schleswig-Holstein decided a similar case.

In this case, however, the university had not included the possibility of recording in its statutes and had only stipulated audio-visual transmission without storing the material. The application for interim legal protection brought forward against this by a student of the university was unsuccessful as well. Here, too, the Higher Administrative Court recognised the suitability of video supervision for the prevention of attempts at deception within the framework of the public interest arising from Art. 6(1)(e) DS-GVO. In addition, the statute was also measured against the standard of the German Basic Law (*Grundgesetz*), but without finding a violation.

Higher Administrative Court of Thuringia, judgment 4 KO 395/19 of 25 March 2021.

In this case, the court had to deal with the question of whether the introduction of electronic university elections requires an explicit legal authorisation.

In this case, the plaintiff was challenging an election held online at a university in 2014. This took place with the software of an external company and in compliance with certain security precautions (registration with personal identification number, possibility of postal voting). The counting of both the online election and the absentee ballots took place publicly in the election office. The plaintiff objected that there was no sufficient legal basis for the procedure. An authorisation in the statutes (*Satzung*) did not meet these requirements. In its ruling, the Higher Administrative Court of Thuringia stated that the legal basis in the university's statutes was sufficient. An explicit legal authorisation is not required. In addition, restrictions of individual electoral principles, which arise when an election is conducted online, can be justified if other principles are thereby strengthened, costs can be saved and voter turnout can be increased. However, within the framework of the statutes, care must be taken to ensure that restrictions on electoral principles are reduced to a necessary minimum. In this regard, balancing act is party responsibility authorized to adopt the bylaws, in this case the university. However, the court also states that minimum requirements for the online voting system are needed in the bylaws. That is, among others: an authentication procedure, regulations on the involvement of external software companies and their employees, as well as the assurance of personal voting (for example, via the possibility of postal voting). In case on hand, university did not meet these minimum requirements. The claim was therefore upheld by the court.

Security Authorities

Higher Administrative Court of North Rhine-Westphalia, decision 16 B 1733/19 of 28 July 2021.

In this case, the Higher Administrative Court confirmed the Administrative Court of Cologne with regard to the application of the GDPR in the area of national security.

In the context of a security clearance procedure against him, the applicant had requested information on the personal data processed, relying on the right to information under Section 15(1) and (3) of the GDPR. After the refusal by the authority, the applicant went to the Administrative Court for interim legal protection. There, his application was rejected. In its decision, the Higher Administrative Court of North Rhine-Westphalia confirmed the decision of the Administrative Court of Cologne. Accordingly, the direct application of the General Data Protection Regulation is excluded here. Pursuant to Article 2(2)(a) of the GDPR in conjunction with the 16th recital of the Regulation, the GDPR does not apply if personal data are processed in an area which does not fall within the scope of Union law. The security clearance procedure is in the area of national security. This is a matter of exclusive competence of the Member States. The applicant can therefore not rely on the GDPR, nor on the European Charter of Fundamental Rights. The latter follows from Article 51 (1) of the Charter of Fundamental Rights.

Electronic patient data

Federal Social Court, judgment B 1 KR 7/20 R of 20 January 2021.

The Federal Social Court has dealt with the question whether the electronic health card of the health insurance companies is compatible with European data protection law.

The electronic health card was comprehensively introduced in Germany in 2015. It primarily stores patients' administrative data electronically. In addition, electronic health card contains a photograph of the patient. In the case on hand,

the plaintiff did not want to provide a photo for the electronic health card and asked the health insurance company to issue a paper proof of insurance instead. This was refused by the health insurance company. The action then brought before the Social Court was unsuccessful. The Federal Social Court also rejected the plaintiff's appeal. There are no concerns about electronic health card regarding data protection and data security. In particular, the card complies with the GDPR. The court leaves open the question of whether the GDPR applies to patient data at all, since at least no breach of the GDPR is apparent. Also, in the area of data security, the legislator had taken sufficient precautions to ensure adequate security with the corresponding regulations (Patient Data Protection Act and corresponding regulations in the fifth German Social Code).

OBLIGATIONS OF ELECTRONIC COMMUNICATION

Administrative Court Würzburg, judgement W 8 K 20.814 of 18 January 2021.

The administrative court determined that there was generally no legal entitlement to the Corona emergency aid (Corona-Soforthilfen) that was not applied for electronically.

In Germany, in the context of the closures of shops and cultural institutions caused by the Corona pandemic, an aid programme was set up to provide rapid financial support to those affected. The application for this aid was possible via a corresponding online portal. The plaintiff requested this support from the aid programme without submitting the electronic application. He was informed several times that the application could not be processed further because the application was only possible online. He then filed a suit at the administrative court alleging 'technological discrimination'. He claimed that he had neither Internet access nor an e-mail account. The court dismissed the complaint. Here, the guidelines for distributing relief funds specify electronic form. This was also possible within the framework of substantive law and, above all, did not violate the 'principle of non-formality' of the administrative procedure. Moreover, it is a matter of voluntary assistance by the State, to which there is no legal entitlement. There is therefore no right to apply for that assistance in a way other than that laid down. It is true that the authorities have some margin of discretion if the applicant can demonstrate the impossibility or unreasonableness of submitting the application electronically. However, general reasons such as a lack of internet connection are not sufficient for this.

ITALY

edited by
Alessandro DI MARTINO, Ph.D. Student in Law Economics at University of Naples Federico II
Elio GUARNACCIA, Administrative Lawyer
Martina INTRONA, Ph.D. Student in General Theory of Trial at University Lum Giuseppe Degennaro

APPLICATION OF PERSON CONCERNED RIGHTS IN A PUBLIC COMPETITION

Regional Administrative Court of Campania, Napoli, sec. VI, n. 8050 of 17 December 2021.

The Regional Administrative Court of Campania, with the case in analysis, has recognized the openness of the native digital files, relating to the tests and the related papers of a public competition, in original and complete version, when a competitor who participated in the same selection makes a request for access to documents under Law no. 241/1990.

In this ruling, the applicant, a competitor in a special competition for the recruitment of secondary school teachers, has challenged, together with the related documents, the acknowledgement of her request for access to documents, pursuant to Law no. 241 /1990, in the part in which the Administration requested, for the display of documents in paper format, the payment of additional costs other than those of mere reproduction or the amount of € 1.00 per page to conceal personal data and has, therefore, contextually denied access to the native digital files of the papers of the other candidates.

Specifically, candidate applied for access to documents, with extraction of the native and digital files, in order to verify the existence of any profiles of illegitimacy vitiating the procedure, so as to be able to take the appropriate legal remedies.

The Administration, on the other hand, invoking certain confidentiality requirements regarding the data of the other candidates, responded to the applicant's request by clarifying that, although she had the right to see the documents, they would be made available in paper format, subject to payment of a fee, in order to make omissions to conceal the data relating to the other competitors.

The Board, with this ruling *de qua*, accepted the appeal on the basis of the following reasons.

With regard to the *an*, it held that, in application of the general principles of impartiality and transparency of administrative action, as well as *favor partecipationis*, access to administrative documents, pursuant to Law no. 241/1990, may be denied only in the individual cases identified in art. 24 paragraphs 1, 2, 3, 5 and 6 Law no. 241/1990 which, however, do not fall into the cases, defined as "exceptions", of the so-called "defensive access", pursuant to art. 24 paragraph 7 Law no. 241/1990. Therefore, in the case in question, the Regional Administrative Court clarified that the applicant, being a participant in the same competitive procedure, has a "direct, concrete and current" interest (art. 22, paragraph 1, Law no. 241/1990), founding its right to access the requested documents.

With regard to the *quid*, with the pronouncement *de qua*, the College - which has preliminarily excluded the possibility of recognizing any other party to the ostension of acts inherent in that procedure, given their inability to affect any subjective legal position - has confirmed the prevailing case law according to which, when a potential candidate decides independently to submit an application for a public competition, it is necessary to recognize his implicit willingness to allow the full disclosure of his application to participate or of the tests and papers incurred and prepared for that purpose, even if possibly subject to the claim of another competitor, aimed at verifying the proper conduct of the procedure. This is confirmed, according to the College, by the conduct of the same oral tests of the competition, to be held in public session, and, therefore, in a manner ontologically incompatible with the prerogatives of confidentiality complained of by the respondent.

With regard to the *quomodo*, Campania Regional Administrative Court, reiterating that there are no particular confidentiality requirements that cannot be overcome by the defensive requirements of the applicant, did not identify any reason against the disclosure of the digital documents requested in their native format, in order to ensure their completeness or their complete consistency with the logical process followed by the jury. On the contrary, it acknowledged that only the display of the documents as they originated would allow the candidate to have knowledge of the real work of the Administration in the competition, also in order to seek any judicial remedies.

Ultimately, Board concluded that the contested notes were illegitimate insofar as they requested, in order to allow the disclosure of documents in paper format, the payment of additional costs to conceal personal data and, therefore, at the same time denied access to other candidates native digital files.

At the same time, pursuant to art. 116, paragraph 4, and art. 133, paragraph 1, no. 6, of the Code of Administrative Procedure, the Campania Regional Administrative Court ordered the requested body, condemning it to pay the costs of the proceedings, to produce the documentation requested by the appellant, also allowing her to extract, in full format, without omissions, a copy of native digital files as requested, without the payment of the costs indicated in the contested deeds, within thirty days from the date of the hearing.

Regional Administrative Court of Emilia-Romagna, Bologna, sec. I, ord. 28 November 2021, n. 551.

The exclusion from a public competition - for the invalidity of the QR Code for the verification of the green pass - is unlawful where it is possible to prove possession with a document certifying the vaccination. Otherwise, the exercise of a constitutionally guaranteed right (Articles 33 and 34 of the Constitution) such as the right to study or access public offices (Articles 51 and 97 of the Constitution) would be conditioned by the operation of a mobile application.

Emilia-Romagna Regional Administrative Court void administrative decision by which the applicants were excluded from in admission test to the Bologna University's degree course in Medicine and Surgery for academic year 2021/22. The University justified its decision because the QR Code showed that the Green Pass was not valid, even though the applicants had proved that they had been vaccinated on 10 August 2021. Although Article 13 of the Prime Minister's Decree of 17 June 2021 states that "the verification of COVID-19 green certificates is carried out by reading the two-dimensional bar code", the Administrative Judges consider that a certificate attesting to vaccination can remedy this "computer error". Otherwise, the exercise of a constitutionally guaranteed right (Articles 33 and 34 Const.) such as the right to study or access public offices (Articles 51 and 97 Const.) would be conditioned by the operation of a mobile application.

ELECTRONIC NOTIFICATION

AgID Guidelines on National Index of electronic addresses of individual citizens, companies and entities that are not required by law to sign up on professional lists, books and registers or in the Register of Companies.

The Guidelines at issue regulate the implementation and the management of the National Index of digital domicile, elected by individuals, professionals, and other institutions that aren't required by law to have a digital address. The real beginning of the index, in short called INAD, will allow every individual or organization to have an effective electronic address for notifications that hold legal value.

The index is covered by the Article 6-quater of Codice dell'Amministrazione Digitale at legislative decree n. 82/2005, along with other indexes of electronic addresses that are already operating.

These other indexes are filled with electronic addresses of Public Administration (INDICEPA and RegistroPA) and professionals and companies that are required by law to have an electronic address, and that are required to sign in professional and companies registers.

As regards INAD, the mentioned article 6 - quater states that the implementation and management of this index are on AgiD, through the issuing of specific guidelines, that the Agency released on 2021 September 15th.

In accordance with law and guidelines, the overmentioned subjects could indicate their own electronic address, by authenticating in a dedicated web platform, using SPID, CNS, and Electronic ID Card.

After the authentication process, people could choose their digital address, by providing a certified e-mail (PEC) address or another electronic registered delivery address for communications holding legal value.

From this moment, they can log in and see their personal data and address.

The chosen electronic address can be deleted in every moment, and, after the deletion, the system stores only the necessary data for the event of a trial.

Organizations and entities can choose their electronic address through their legal representative, and they can also choose a delegate.

The Guidelines state that individuals may elect two different electronic addresses, one for their professional activity and one for personal purposes.

The Guidelines also plan the connection between the information contained in the Index and ANPR (national database of residing people's data).

Therefore, on a daily basis, the electronic addresses of the INAD flow to ANPR, once complete.

The Index will also collect the electronic addresses of professionals and companies that are required by the law to have an electronic address and that are signed up on registers.

These electronic addresses, which are already listed in INI PEC index, flow also into INAD.

Anyway, the Guidelines state that these professionals and companies can choose a different personal electronic address and put it into the INAD.

Concerning the consultation of the index, Guidelines require that users can search electronic addresses by putting into the website search engine the fiscal code or the electronic address of the called subject.

PORTUGAL

edited by

Luís Manuel PICA, PhD candidate in Public Law at The University of Minho (Portugal). Teaching assistant at the Polytechnic Institute of Beja (Portugal) and researcher at JusGov- Research Centre for Justice and Governance at University of Minho (Portugal)

Mário Filipe BORRALHO, Master's student at Law School - University of Lisbon (Portugal); Solicitor; Teaching assistant at the Polytechnic Institute of Beja (Portugal)

THE ELECTRONIC NOTIFICATIONS IN THE ADMINISTRATIVE TAX OFFENCE PROCEEDING

Judgment of the Administrative Court of appeal (south) 30 September 2021.

If the notification is sent to the digital electronic mail address (i.e. the electronic tax domicile: "ViaCTT"), the addressee is presumed to have knowledge of it, unless the notifying party proves that, for reasons beyond its control, the notification took place after the presumed date and if it is proved that the party communicated the change of address within the time limit and in the manner provided for in Article 43 (Art. 39(11) CTPP).

In this ruling, the South Central Administrative Court (SCAC) - one of the two intermediate courts of administrative and tax jurisdiction in Portugal - addressed the issue of the validity and

perfection of electronic notifications made to the defendant in administrative tax offence proceedings. It's basis is an administrative decision (by a tax service) to impose a fine on the defendant. Dissatisfied, the defendant appealed to the Administrative and Tax Court (ATC). Because the appeal had formal deficiencies, the court gave the defendant ten days, by order sent by electronic notification to his electronic domicile, to remedy the deficiencies, failing which the application would be outright rejected. Upon expiry of the deadline without having remedied the deficiencies, the defendant wanted to challenge the decision (of the ATC) to dismiss the appeal, claiming that he had not been notified of the aforementioned order.

In this case, the judges of the SCAC analyzed the concept of tax domicile, reformulated in 2017 by the amendments made by Decree-Law no. 93/2017, of 01/08, to article 19(2) of General Tax Law (GTL), which enshrines the electronic tax domicile, that includes the public service of electronic notifications associated with the digital single address (an email address indicated by the taxpayer when registering in the system) and the public service of electronic mailbox (called "ViaCTT", an electronic mailbox that works as a digital mail receptacle - also requires adherence by the taxpayer).

Reflecting such innovation, the article 39(10) of the Code of Tax Procedure and Proceedings (CTPP), in the wording in force at the time of the facts, stipulated that notifications sent to the electronic tax domicile were deemed to have been served on the fifth day following the registration of their availability in the support system of the public electronic notifications service associated to the single digital address or in the electronic mailbox of the person to be notified. Thus, the judges considered that since the notification was sent to the electronic address, it is presumed that the addressee became aware of it. This presumption may only be rebutted by the notifying party when, for reasons not attributable to him, the notification occurs on a date subsequent to the presumed date and in cases where it is proven that the he communicated the change of address within the time periods and terms set forth in article 43 (article 39(11) of CTPP).

Judges of the SCAC also determined that, since electronic notification could only be made if the defendant had previously subscribed such services - digital single address or electronic mailbox -, he could not ignore the duty of care regarding their monitorization, as well as that, by ensuring the way to counter such iuris tantum presumption, the legislator ensured the most elementary rights of defense to those notified. They concluded that no facts emerged from the case file that would allow the defendant not to be considered as having been notified of the order inviting him to remedy the formal deficiencies of the appeal brought before the ATC, and that the ruling of this court (in rejecting the appeal outright) does not delay his right of access to the courts and the guarantee of effective judicial protection. The appeal was dismissed.

PERSONAL DATA IS SHARED BETWEEN THE PUBLIC ADMINISTRATION AND PUBLIC ENTITIES.

Judgment of the Administrative Supreme Court of 23 June 2021.

In accordance with the principle of loyal cooperation between public administrations, the Portuguese Administrative Supreme Court held that the limitation of other public bodies' right of access to personal data, when an inter-administrative protocol is concluded, does not violate the constitutional right of access to administrative information.

The decision concerns the identification and data that taxpayers must provide to the Tax Administration. Taxpayer identity components given in processes for the allocation and administration of the tax identification number, according to this court, comprise personal data protected by tax secrecy. The characteristics indicating the tax residence of taxpayers should be subject to the confidentiality laws controlling administrative activities since they are personal data covered by tax secrecy.

However, where law allows Tax and Customs Administration to cooperate with other public institutions and to the extent of its capabilities, the obligation of tax confidentiality does not preclude such data from being shared with them. Among these responsibilities, it is important to note that circumstances in which the Tax and Customs Administration cooperates with other public institutions are those in which the law allows for cooperation implementation protocols between these entities. Article 23, paragraph 2 of Law 58/2019 mandates the execution of protocols between public organizations for personal data communication.

That court therefore held that restricting the right of access of other public entities to personal data to cases where inter-administrative protocol is concluded does not offend the constitutional right of access to administrative information.

THE ELECTRONIC SIGNING OF DOCUMENTS IN THE PORTUGUESE PUBLIC CONTRACT LAW

Judgment of the Administrative Supreme Court of 25 November 2021.

Case law requires the signature on each document even if it is incorporated in a single PDF, considering the PDF signature alone to be insufficient, and sanctioning this omission with the exclusion of the participant.

The Portuguese public contract law has evolved towards a focus on information technology, which provides better communication and more effective, efficient and transparent processes (fundamental in the management of public money), and also increasing the possibility of economic operators participating in tenders throughout the internal market. Thus, the documents necessary for the formation of public contracts - such as the proposal and respective supporting documentation - are submitted through an electronic platform used by the contracting entity, by means of written and electronic data transmission (articles 57(4), and 62(1) of Public Contracts Code). They must be signed with a qualified electronic signature (using certificates issued by entities on the Trusted-Service Status List, namely the one on the citizen card - articles 54(1), and 69(1) of Law no. 96/2015, of 17 August).

In this ruling, and standardizing jurisprudence on an issue that has been an important and controversial topic in the Portuguese administrative courts, the Supreme Administrative Court considered that the electronic signature must be individually affixed to all documents submitted, so that submission of a proposal in a single digitally signed PDF file that grouped several autonomous documents not signed electronically does not meet the requirement of individualized signature of each document imposed by the aforementioned precepts. In order to support such understanding, it was argued that only through the qualified electronic signature of each document of the proposal is it possible to ensure the binding of all its elements, as required by law, and that, although they are different realities, the treatment to be given to the "grouped document" (which results from the junction of several other documents in a single document) should be the same as that given to the compressed file (which results from the compression of several files - such as, for example, ZIP folders - and which the law and prevailing jurisprudence understand must also be signed individually).

ELECTRONIC NOTIFICATIONS FROM THE TAX ADMINISTRATION

Judgment of the Administrative Court of Appeal (South) 7 December 2021.

The computer 'printouts' prepared by the tax administration for internal purposes do not prove the reality of the facts referred to therein and thus the notification to the addressee, however, the failure to register the registered letter as required by law does not invalidate the notification when it can be proved that the addressee became aware of the notified document despite the failure to comply with this formality.

The documents issued by the Tax and Customs Administration cannot be used to demonstrate that the Contestant was notified of the tax and interest settlements via electronic means (via CTT), because such computer "prints" are prepared by the Tax Administration for internal purposes and do not prove the facts reality referred to in them.

The purpose of the law's requirement of a registered letter is achieved when it can be proven that the addressee has become aware of the notified document despite the failure to comply with that formality, so that the formality of the registered letter is degraded to non-essential, and the notification is not invalidated. Consequently, even if the Tax and Customs Administration does not follow all the formalities of notifying the receiver of the tax due, the tax should not be cancelled since the breach of the legal precept does not result in any genuine, actual harm to the interests protected by the legal precept.

SPAIN

edited by
Javier MIRANZO DÍAZ, Professor Lector in Administrative Law at The University of Castilla-La Mancha.
Alfonso SÁNCHEZ GARCÍA, Professor Lector in Administrative Law at The University of Murcia.

PROCEDURAL RIGHTS AND OBLIGATION TO USE ELECTRONIC CHANNELS

Supreme Court (Tribunal Supremo), Contentious-Administrative Chamber, Third Division, case 954/2021, 1 July 2021, appeal number 1928/2020.

Article 68.4 of Law 39/2015 is only applicable to administrative procedures launched by applicants, but not to those unilaterally initiated

by public authorities or to procedures for the revision of administrative acts.

In this Ruling, the scope of Article 68.4 of Law 39/2015, of 1st October, on Common Administrative Procedure of Public Administrations, is analysed when the obligation to use electronic means imposed by Article 14.2 has not been complied with; the aforementioned defect is subsequently remedied.

Despite the meaning of the provision not being expressly defined, it is considered by the lower court judgment under appeal as not contradicting the fact that, in the case of proceedings against administrative acts, such rectification is retroactive when taking into account the date on which the appeal was submitted and, therefore, whether or not the time deadline for submitting the appeal has been observed.

The Supreme Court concludes that the approach of the lower court is correct since article 68.4 of Law 39/2015 regulates a remedy that is applicable only to procedures launched on request of the person concerned and not to those initiated *ex officio* by the Administration nor to procedures for the review of administrative acts. Therefore, an interpretation that would imply the general application of the aforementioned provision to any type of procedure would be contrary to the principle of Good Administration and would entail an infringement of the constitutional right to due legal procedure.

Supreme Court (Tribunal Supremo), Contentious-Administrative Chamber, Third Division, case 1263/2021, 25 October 2021, appeal number 706/2020.

The issuing of a digital certificate to a natural person by a public sector provider for the purpose of representing a legal body implies the recognition a representation capacity that cannot be questioned by another administrative authority and that would potentially involve the faculty to lodge appeals.

The Regional Administration of Galicia required a citizen to submit a correction of his appeal using electronic means and to provide the formal accreditation of the company's representation. Within the period granted for the remedy, the interested party submitted by electronic means a mere digitalised copy of the formal paper-based document, in which the company's decision to appoint a representative was confirmed, but the amendment was rejected.

The Supreme Court understands that according to art. 5.4 of Law 39/2015, the means of proof of representation cannot be determined solely by the Administration. The Supreme Court states that the representation granted by a Notary cannot be refused merely on the grounds that it has not been digitally signed, as it was originally in a paper document, and has not been digitalised at the Administration's official website. It also states that prior to the issuance of a digital certificate to act on behalf of a legal person by a public sector provider, it must be verified that the natural person requesting it has the corresponding entitlement to act as its legal representative. Therefore, this representation cannot be questioned by another authority when a particular action is performed.

ELECTRONIC NOTIFICATIONS

Supreme Court (Tribunal Supremo), Contentious-Administrative Chamber, Third Division, case 1320/2021, 10 November 2021, appeal number 4886/2020.

The final day (dies ad quem) of a procedure for the purpose of the expiry date in electronic procedures.

The initial dispute arose around the appeal filed by Galeón Software S.L. against the resolution of the Secretary of State for the Information Society and Digital Agenda, of 4 July 2017, which agreed to the total reimbursement for non-compliance with the state aid granted in the 2010 Strategic Action of Telecommunications and Information Society call (file TSI-020100-2010-1032).

The administrative procedure for reimbursement was initiated on 7 July 2016, and the deadline for issuing a decision was of 12 months. The notification of the initiation of the procedure was made available by the Administration on the official electronic side on 7 July 2017. However, the enterprise concerned did not access the notification until 10 July 2017.

The first instance court interpreted that the reimbursement procedure had expired, by exceeding the maximum period of 12 months to resolve and notify the resolution of the procedure from the date of the initiation agreement, established by article 42.4 of 38/2003 Act for State Aid.

It is accepted by all parts that the notification of the final decision of the reimbursement procedure on 7 July 2017, was within the maximum period of 12 months established by article 42.4 of 38/2003 Act to resolve and notify the resolution. Consequently, the judgment under appeal focuses the disputed issue on deciding whether the end of the procedure can be assimi-

lated with the date in which the notification is made available to the appellant (in this case 7 July 2017), or with the date of effective access to its content by the individual concerned (in this case 10 July 2017). The answer to this question is decisive for the declaration or not declaration of the expiry of the procedure.

The Supreme Court has ruled a number of judgements in which it sets out a clear criterion for paper-based or traditional notifications. In these cases, the court understands that article 40.4 from the 37/2015 Act states that the attempt of notification by any legally admissible means, with all the legal guarantees, implies the fulfilment of the obligation of the Administration to notify within the maximum period of duration of the procedures. Therefore, even when this notification attempt is finally frustrated, if it is duly recorded and accredited, it precludes the expiry of the procedure.

The central point of this judgement is whether this applies to electronic procedures, and if so, if the uploading of the notification in the official site can be considered as a valid attempt of notification with equal consequences as paper-based ones.

The Court concludes that the attempt of notification shall be understood to have been complied with the legal requirements –for expiry purposes– with the uploading of the notification in the electronic site of the Administration or Acting Body. Therefore, the final decision of the reimbursement procedure was issued and made available to the appellant at the corresponding electronic site on July 7th, 2017, that is, within the period of the year established by law.

PUBLIC PROCUREMENT ELECTRONIC SUBMISSION

Decision from the Tribunal Administrativo Central de Recursos Contractuales (Administrative Independent body), decision 813/2021, 1 July 2021.

Incompatibilities with the submission webpage software cannot be alleged as platform errors.

The claimant submitted a bid to a public procurement procedure out of the specified timeline invoking technical problems with the platform. However, the contracting authority, as of May 11th, 2021, agrees not to accept its offer for being extemporaneous.

In this case, the company claims that it has not been demonstrated that the lack of presentation is consequence of an incident or mistake attributable to the company. Likewise, it understands that the contracting authority was aware of the technical incident, and it did not take any step aimed at solving it or allowing the correction of the defect which prevented the presentation of the bid in a timely manner.

The previous case-law of the court had established that for the extension of the term or the admission of offers to be appropriate, it is essential that the affected company 'proves the impossibility of presenting offers through the Public Sector Contracting Platform' (in general, or the platform or computer application used in each case), and that the technical problems were not attributable to the tenderer itself (see for example, resolutions 1178/2018, 560/2018 and 595/2018 of the Tribunal Administrativo Central de Recursos Contractuales).

In this case, it is clear from the report prepared by the Department of Quality, Security and Legal of Vortal (company in charge of the platform) that the problems experienced by the bidder were due to the type of browser used, as proves the fact that after changing the browser, according to the indications of the Vortal support centre, they could submit it without technical problems, although then out of the specified timeline.

Since the aforementioned incompatibility of browsers was already warned in Annex VII of the procurement documents under the heading `Information about the Electronic Bidding Platform of the Corts Valencianes', the court considers that the fault is attributable to the appellant, and therefore its offer cannot be admitted in the procedure due to extemporaneity in the presentation.

DATA PROTECTION

Supreme Court (Tribunal Supremo), Contentious-Administrative Chamber, Third Division, case 344/2021, 11 March 2021, appeal number 8040/2019.

In this ruling, the Supreme Court analyses whether a local Council can use tax data obtained in the context of a criminal case as lawful evidence for other administrative enforcement purposes (infringement of taxi regulations).

The court bases its decision on Article 95.1 of the General Tax Law, which establishes a concrete application of the general principles of data protection. According to this provision, while there is a specific legal authorisation for the communication of tax data to a court, this is not the case if such data is requested by another

public administration for the exercise of competences other than those relating to taxation.

Although the City Council concedes that it had initially become aware of the data in a criminal proceeding in which it was involved, given that the data had been provided by the State Tax Agency to a court for the exercise of its judicial functions, there was not sufficient legal basis to use it. For this reason, it requested the data directly from the Agency, which supplied it with the condition that it was to be used for the exercise of taxation powers. Nevertheless, the City Council used the tax data to impose a sanction in applying the taxi enforcement regulations.

According to Article 58.2 of Royal Decree 1065/2007, when a Public Administration requests the transmission of tax data by electronic means, the data required, their owners and the purpose for which they are required must be identified. In addition, the express consent of the affected data subject has to be previously obtained if there is no legal authorization. Consequently, the Supreme Court concludes that if the City Council aims to use the information for the exercise of functions other than taxation and there is no legal rule that allows for the data transfer, the authorisation of the interested individual must be obtained, thus annulling the sanction imposed by the City Council.

Agencia Española de Protección de Datos (AEPD, Administrative Independent body), decision E/12482/2021, 2 November 2021.

Contract for the processing of personal data for the use of the Teams platform.

Article 28.3 of the Regulation 2016/679 states that the processing of personal data by a processor shall be governed by a contract or some other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject matter, duration, nature and purpose of the processing, as well as the type of personal data and categories of data subjects and the obligations and rights of the controller.

Similarly, the European Data Protection Board guidelines 7/2020 has stated that these requirements shall consider the following:

Unwritten agreements (regardless of how comprehensive or effective they are) cannot be considered sufficient.

The contract or another legal act under Union law or the law of the Member States should be binding on the processor with respect to the controller, i.e., it should establish binding obligations for the processor.

In this particular case, the subscription to Microsoft services took place electronically on 17 December 2014, and initially contained no provisions regarding the processing of personal data. However, a subsequently amendment was made with additional conditions of data processing and standard clauses as guarantees for international data transfers was completed in the first quarter of the 17-18 academic year, with automatic annual renewal. It is accredited that there is a data processing contract –even if it is an amendment and it was signed later– of OFFICE 365 Education with MICROSOFT.

Agencia Española de Protección de Datos (AEPD, Administrative Independent body), decision PS/00128/2020, 25 February 2021.

The fingerprint check must be notified to the employee in a complete, clear, concise manner.

The processing of this data is expressly permitted by the GDPR when the employer has a legal basis. In cases such as the attendance monitoring, the employment contract itself has been interpreted as the enabling element. In this regard, the previous case-law from the Spanish Supreme Court (see case 5017/2003, July 2nd 2007) has accepted the processing of biometric data carried out by the Administration for the time control of its public employees, without the requirement of prior consent from the workers.

However, the following requirements should be met:

The worker should be informed about these treatments.

The principles of purpose limitation, necessity, proportionality, and data minimisation should be respected.

The biometric system used and the security measures chosen shall ensure that the re-use of the biometric data in question for another purpose is not possible.

Mechanisms based on encryption technologies shall be used to prevent the unauthorised reading, copying, modification or deletion of biometric data.

Biometric systems shall be designed in such a way that the identity link can be revoked.

A choice should be made to use specific data formats or technologies that make it impossible to interconnect biometric databases and unproven data disclosure.

Biometric data should be deleted when they are not linked to the purpose for which they were processed and, if possible, automated data deletion mechanisms should be implemented.

In the present case, an Impact Assessment

form was carried out on the processing of fingerprint data for employee presence control. Likewise, there was a security document on the fingerprints of the workers, and all the necessary guarantees were *a priori* fulfilled according to the law.

However, the Data Protection Agency identifies a deficiency in the duty to inform the employee. Thus, in relation to the questions raised in the present case, it should be noted that the implementation and integration of a time control system based on fingerprints by the employer must be informed to the employees in a complete, clear, concise manner. In addition, the aforementioned information must be completed with reference to both the legal bases that cover that type of access control and the basic information referred to in Article 13 of the GDPR.

In the case under consideration, there is no record of the respondent's response to the letter submitted by the complainant requesting information on the time when the information was provided to the workers of the fingerprint registration system. Therefore, it is evident that the defendant has not adequately reported the control of presence and access to its municipal facilities through a fingerprint system. Therefore, it is evident that the defendant has not adequately reported in relation to the control of presence and access to his municipal facilities through a fingerprint SYSTEM.