European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 241-265
ISSN 2724-5969 – ISBN 979-12-218-0798-1 – DOI 10.53136/9791221807981 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

NEW INTEROPERABLE EUROPE ACT TO DELIVER MORE EFFICIENT PUBLIC SERVICES THROUGH IMPROVED COOPERATION BETWEEN NATIONAL ADMINISTRATIONS ON DATA EXCHANGES AND IT SOLUTIONS

Proposal for a Regulation of the European Parliament and of the Council laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act)

The European Commission has proposed a Regulation on the interoperability among public sector entities across the EU.

The European Commission has published the legislative proposal known as the Interoperable Europe Act, along with its accompanying Communication (18 November 2022).

The initiative aims to enhance collaboration and interoperability among public-sector entities across the European Union. The Act's main goal is to establish a network of interconnected digital public administrations that are, at the same time, independent and linked to each other. This effort will expedite the digital transformation of the public sector in Europe and contribute to the provision of improved public services to individuals and businesses.

Indeed, the digitization of public administrations is a key focus for this decade, and Member States are heavily investing in modernizing their public sector through digital means. However, despite the increasing number of digital services offered by the EU public sector, there is still a lack of adequate interoperability among them. In this regard, it is written down in the proposal that the Commission can 'set up projects to support public-sector bodies in the digital implementation of Union policies ensuring the cross-border interoperability of network and information systems which are used to provide or manage public services to be delivered or managed electronically ("policy implementation support project") (Art. 9, para 1).

By achieving these objectives, the Act plays a crucial role in attaining Europe's digital targets for 2030 and facilitating the smooth flow of trusted data. Additionally, implementing cross-border interoperability has the potential to generate significant cost savings. It is estimated that citizens could save between €5.5 and €6.3 million, while businesses engaged in transactions with public administrations could save between €5.7 and €19.2 billion.

From a first reading of the proposal, two possible advantages can already be pointed out:
a) The proposal backs the establishment of a governance model for this policy, comprising two principal entities - the Interoperable Europe Board and the Interoperable Europe Community;
b) The Act includes provisions for developing experimental solutions that facilitate collaborations between the public sector and innovative-technology companies and startups. The aim is to foster the creation of pioneering experimental solutions that can be implemented and shared across public services.

EUROPEAN DIGITAL IDENTITY (EID)

European digital identity (eID): Council makes headway towards EU digital wallet, a paradigm shift for digital identity in Europe

The revised Regulation seeks to guarantee universal access to secure and reliable electronic identification and authentication for individuals and businesses. This will be achieved through the use of a personal digital wallet on a mobile phone.

The Council has approved its common position on the proposed legislation concerning the framework for a European digital identity (so called 'general approach' – 6 December 2022).

In June 2021, the Commission put forth a framework for a European digital identity (eID), aiming to provide access to all EU citizens, residents, and businesses through a European digital-identity wallet (Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity - COM(2021) 281 final, 2021/0136(COD) – 3 June 2021, available on:

eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281.

The proposed framework entails modifications to the 2014 Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). The eIDAS regulation established the groundwork for secure access to public services and online transactions within the EU, both domestically and across borders.

The Council welcomed the EC's proposal to amend the eIDAS Regulation, as the revision aims to adapt the existing legal act to meet current market requirements. The Council stated the necessity to enhance digital-service solutions, ensuring broader access for both private and public sectors, as the goal is to make these solutions accessible to a significant majority of European citizens and residents. Indeed, the revision intends to achieve that at least 80% of European citizens should be able to use a digital ID solution to access key public services by 2030.

The ball is now in the European Parliament's court.

The hope is that, in the final draft, effective data protection will be looked at in the context of the protection of fundamental rights, in particular the right to privacy and the right to the protection of personal data, as already underlined Opinion of the European Economic and Social Committee on the proposal (COM(2021) 281 final – 2021/0136 (COD) – 20 October 2021, available on: eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021AE2756.

Indeed, the digitalization process, particularly the development of large-scale systems that store and process data, raises numerous security concerns regarding the vulnerability to fraud and data loss. Currently, e.g., there is no security system capable of providing comprehensive data protection. In light of this, the EESC already emphasized that users of European Digital Identity Wallets should be provided with assurance of compensation in the event of any adverse situations concerning their data, such as data theft or unauthorized disclosure. This liability should be strict, i.e. independent of whether the service provider is at fault.

THE COURT OF JUSTICE DECLARES A PROVISION OF THE ANTI-MONEY LAUNDERING DIRECTIVE INVALID FOR BEING CONTRARY TO THE CHARTER OF FUNDAMENTAL RIGHTS

Court of Justice of the European Union (CJEU) (Grand Chamber), Judgment of 22th November 2022, Joined Case C-37/20 e C-601/20, WM Sovim and SA v. Luxembourg Business Registers - Request for a preliminary ruling under Article 267 TFEU from the Tribunal d'arrondissement de Luxembourg, made by decision of 24 January 2020.

The Court of Justice declared invalid, in light of the Charter, the provision of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, pursuant to which Member States shall ensure that information on the beneficial ownership of companies and other legal entities incorporated in their territory is accessible to the public in all cases. In the Court's view, public access to beneficial-ownership information constitutes a serious interference with the fundamental rights to respect for private life and the protection of personal data, respectively enshrined in Articles 7 and 8 of the Charter. Indeed, the information disclosed allows a potentially unlimited number of persons to find out about the beneficial owner's material and financial situation. Moreover, the potential consequences for the persons concerned of any misuse of their personal data are aggravated by the fact that, once made available to the public, such data may not only be freely accessed, but also stored and disseminated.

Two appeals were brought to the EU Court of Justice by a Luxembourg company and the beneficial owner of a Luxembourg company, respectively, who had unsuccessfully requested the LBR to restrict public access to information about them. The two companies considered that the disclosure of that information was likely to entail a disproportionate risk of infringement of the fundamental rights of the beneficial owners concerned, and therefore, the court referred a number of questions to the Court of Justice for a preliminary ruling concerning the interpretation of certain provisions of the Anti-Money Laundering Directive and the validity of those provisions in light of the Charter of Fundamental Rights of the European Union.

It should be pointed out, that in accordance with the Anti-Money Laundering Directive, a Luxembourg law adopted in 2019 established a Register of Beneficial Owners, providing that a whole range of information on the beneficial ownership of registered entities must be recorded and stored therein. Part of this information is accessible to the public, in particular via the Inter-

net. That law also provides for the possibility for a beneficial owner to request the Luxembourg Business Registers (LBR), the manager of the Register, to restrict access to that information in certain cases.

In its judgment, the Court of Justice declares that the provision of the Anti-Money Laundering Directive under which Member States shall ensure that information on the beneficial ownership of companies and other legal entities incorporated in their territory is accessible to the public in all cases infringes upon the Charter.

In the Court's view, public access to beneficial ownership information constitutes a serious interference with the fundamental rights of respect for private life and of protection of personal data, enshrined respectively in Articles 7 and 8 of the Charter. Indeed, the information disclosed allows a potentially unlimited number of persons to find out about the beneficial owner's material and financial situation. Moreover, the potential consequences for the persons concerned of any misuse of their personal data are aggravated by the fact that, once they have been made available to the public, those data may not only be freely consulted, but also stored and disseminated.

The Court notes that the European Union legislature seeks to prevent money laundering and terrorist financing by establishing, by means of greater transparency, an environment less likely to be used for such purposes.

However, the Court finds that the interference resulting from such a measure is neither limited to what is strictly necessary nor proportionate to the objective pursued. In addition to the fact that the provisions at issue in the present case authorise the making available to the public of data which are neither sufficiently defined nor identifiable, the regime introduced by the anti-money laundering directive represents a considerably more serious infringement of the fundamental rights guaranteed by Articles 7 and 8 of the Charter than the previous regime, which provided not only access by the competent authorities and certain entities, but also by any person or organisation that could demonstrate a legitimate interest, aggravation that, however, did not result in any benefits from the new regime as compared with the previous one, from the point of view of the effectiveness of the fight against money laundering and the financing of terrorism.

In particular, the possible existence of difficulties in defining precisely the cases and conditions in which such a legitimate interest exists, relied on by the Commission, cannot justify the fact that the European Union legislature provides for public access to the information in question. The Court adds that the optional provisions enabling the Member States, respectively, to make the provision of beneficial-ownership information subject to online registration and to provide, in exceptional circumstances, for certain exceptions to public access to that information, are not, in themselves, capable of demonstrating either a proper balance between the public-interest objective pursued and the fundamental rights enshrined in Articles 7 and 8 of the Charter or the existence of sufficient safeguards enabling the persons concerned to effectively protect their personal data against the risks of abuse.

DATA RETENTION: TRAFFIC DATA OF ELECTRONIC COMMUNICATIONS FOR CRIME-PREVENTION PURPOSES

Court of Justice of the European Union (CJEU) (Grand Chamber), Judgment of 20th September 2022, Joined Case C-339/20 e C-397/20, VD and SR - Request for a preliminary ruling under Article 267 TFEU from the Cour de cassation - France, made by decision of 1st April 2020.

The Court of justice confirms the "prohibition of generalised and indiscriminate retention" of traffic data of electronic communications for crime-prevention purposes.

In its judgment, the Court was prompted by a reference for a preliminary ruling from the French Court of Cassation, in a case concerning the acquisition - in the context of criminal proceedings for the offences of insider dealing, secondary insider dealing, aiding and abetting, bribery and money laundering - of traffic data retained, for one year, on the basis of the relevant national legislation. The questions raised by the French Court of Cassation concerned, in particular

- the interpretation of the "market abuse" directive and regulation (Article 12(2)(a) and (d), Directive 2003/6/EC and Article 23(2)(g) and (h), Regulation (EU) 596/2014), read in conjunction with Article 15(1) of Directive 2002/58/EC, read in light of the Cdfue and the compatibility, with that framework, of national legislative measures imposing on operators of electronic communication services, a generalised, preventive and indiscriminate retention of traffic data for one year from the day of registration, for the purpose of combating market-abuse offences;
- the admissibility of the provisional effectiveness of domestic legislation, where deemed in-

compatible with European rules, in order to avoid excessive legal uncertainty and to allow the use, for evidentiary purposes, of data retained under such legislation.

Pending the decision of the Court of Justice, moreover, the Conseil d'État (French Data Network and others: nos. 393099, 394922, 397844, 397851, 424717, 424718), by which the national provisions on the generalised retention of connection data for the purposes of justice were declared unlawful, with the exception of the part relating to the retention of IP addresses and data relating to the personal identity of users of electronic communications networks, in line with the CJEU judgment of 6 October 2020, La Quadrature du Net and Others (C-511/18, C-512/18 and C-520/18, EU:C:2020:791).

With the VD judgment, the Court of Justice today declares incompatible with Article 15(1) of Directive 2002/58, read in light of Articles 7, 8, 11 and 52(1) CDFUE, national legislation, such as that at issue, which requires operators of electronic-communications services -for the purpose of combating market-abuse offences- to store the traffic data of all users of electronic communications media in a generalised and indiscriminate manner, 'without any distinction being made in that regard or any exceptions being provided for and without the required relationship, within the meaning of the case-law cited in the preceding paragraph, between the data to be retained and the objective pursued being demonstrated' (paragraph 94). The reference to the previous case law (and, in particular, to the judgment of 5 April 2022) therefore serves to reiterate, albeit indirectly, the parameters for the admissibility of the retention of printouts outlined there, i.e. subjective, geographical or other criteria (provided that they are objective and non-discriminatory) such as to imply a functional relationship between the investigative needs and the data to be acquired.

The Court reiterates, moreover, the inadmissibility of a limitation, in time, of a declaration of invalidity of domestic legislation requiring operators of electronic communications services to retain traffic data generally and indiscriminately and permitting them to be communicated to the competent authority without prior authorisation by a court or an independent administrative authority. Otherwise, the primacy and the need for uniform application of Union law would be undermined.

To quote from the judgment of 2 March 2021, H.K. v. Prokuratuur (C 746-18), the Court further states that the question of the admissibility of evidence obtained pursuant to national legal provisions incompatible with European Union law is a matter of national competence, in accordance with the principle of the procedural autonomy of the Member States, subject, however, to compliance with the principles of equivalence and effectiveness.

With regard to the latter principle, the Court points out that it requires the national court to exclude information and evidence obtained through the generalised and indiscriminate retention of traffic data and location data on the basis of rules incompatible with European Union law, or even through access by the competent authority to such data which is incompatible with European law, where the party against whom that evidence is used cannot 'effectively make its views known on that information and that evidence, which relates to a matter outside the knowledge of the courts and is capable of having a predominant influence on the assessment of the facts' (paragraph 106).

BELGIUM

edited by
Elise DEGRAVE, Professor at University of Namur; Director of research at 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
Kathryn BARETTE, researcher at NADI-CRIDS

DATA PROCESSING BY PUBLIC AUTHORITIES

Belgian Data Protection Authority (BDPA) (Litigation chamber), decision 115/2022 of 19 July 2022

The BDPA had to rule on the question of whether the GDPR allows disclosure of sensitive data during a work meeting.

The BDPA received a complaint concerning the disclosure of personal data relating to an employee's health by her manager during a departmental meeting in which she was not present. First, the contentious chamber identified the data processing in question and recalled that oral communications do not fall within the scope of the GDPR. However, in the case at hand, the oral statements made by the manager were recorded

in the minutes of the meeting. Hence, a data processing under articles 2.1. and 4.1. of the GDPR took place. The decision also confirms that the disclosure of information relating to the claimant constitutes a processing of data relating to health. Second, the BDPA recalled that each processing operation must be based on one of the grounds of lawfulness enshrined in article 6.1. GDPR. Furthermore, as that the defendant processed data relating to the claimant's health, this processing must be based on Article 9.2. of the GDPR read in conjunction with Article 6.1. of the GDPR. In this case, the claimant's complaint was directed against the further processing (i.e the communication during a meeting) of information relating to her health. The litigation chamber decided that, even if the purposes for which the data were originally collected are identified, lawful and legitimate their further disclosure is not compatible with these purposes. Since the defendant is a public authority in respect of whom administrative fines cannot not be imposed the BDPA decided to issue a reprimand.

Brussels Court of Appeal, Brussels Markets Court, 19th Chamber A, judgment of 26 October 2022

An appeal was filed against the decision 31/2022 of 4 March 2022 (already commented in the previous report) of the Belgian Data Protection Authority.

The appealed decision concerned a case in which the claimant had been issued with a parking ticket and subsequently a parking charge. Until 1 January 2020, an autonomous entity of the city of Kortrijk called "the RCO" was authorised to process the vehicles plate number of offenders on the basis of a normative text ("deliberation no. 02/2016"). On 1 January 2020, this entity was dissolved and the city of Kortrijk took over this prerogative. The claimant therefore argued that the city of Kortrijk breached the GDPR when it relied on "deliberation 02/2016" to process his number plate. Unlike the RCO, the city was not the addressee of this normative text. Hence, according to the claimant, at the time of the facts, the City of Kortrijk was not authorised to perform the data processing necessary to identify his vehicle plate number. The City of Kortrijk argued that it was the legal successor of the RCO and was therefore authorised to process the complainant's personal data. The BDPA had considered that a legal succession could take place as long as the purpose of the processing of personal data remained unchanged. The BDPA also found that the city breached GDPR transparency and information requirements. During the appeal, the City (supported by the Federal Public Service Mobility) argued that during the procedure before the BDPA, (1) it was never informed of the exact offences it was accused of and (2) it was never clear against which arguments it could defend itself. In particular, the City argued that it had never been informed that it had breached the transparency requirements under the GDPR (arts. 5.1.a., 12.1. and 14.1.). According to the BDPA, this breach was indeed raised during the proceedings before the litigation chamber. In the Court's view, the elements on which the BDPA relied to allege that the breach of the duty of transparency could be imputed to the City of Kortrijk were not sufficient and that the latter should have been clearly informed of the legal bases on which the BDPA based the breach of its duty of transparency. The Court decided that the BDPA's decision was incompatible with the principles of diligence and fairness, the right to be heard and the right to cross-examine. It therefore ordered the BDPA to review the complaint against the City.

Council of State, judgment 254.571 of 21 September 2022

The Council of State received two actions for annulment of the Brussels regional government's decrees creating low emission zones (LEZ). The citizen who filed the claims relied, among others, on an argument based on the violation of the GDPR.

A citizen filed, before the Council of State, two actions for annulment against the decrees of the Government of the Brussels-Capital Region establishing low emission zones. Adoption of these decrees stems from the Directive 2008/50/EC, which requires Member States to establish zones in which ambient air quality is assessed and to define Low Emission Zones. This implies that access to certain categories of vehicles that emit atmospheric pollutants is restricted in LEZ. The government can however waive the restriction by granting temporary access to the LEZ against payment. Before the Council of State, one of the arguments raised by the applicant is that the government's request to communicate the identity of the driver upon purchase of a LEZ pass, violates the GDPR (art. 5.1 c.). To that extent, the applicant considered that only processing of vehicle plate number was relevant to purchase a pass. On the other hand, other data collected (identity of the driver, identity of the applicant for the pass) were not necessary and were therefore violating the right to privacy.

The Council of State did not follow this argument. On the contrary, the decision highlights that there is no requirement that the purchaser of the pass correspond to the person who will use the vehicle covered by the pass. According to the Council of State, the requirement to state one's identity is a purely formal requirement common to any request filed before an administrative authority. Hence, this data processing does not disproportionately infringe the right to privacy.

Belgian Data Protection Authority (BDPA) (Litigation chamber), decision 186/2022 of 19 December 2022

Two complaints were filed for the disclosure of personal data by the Financial Services and Markets authority (FSMA).

The BDPA received complaints regarding a payment-reminder email sent by the FSMA (the defendant). In particular, this email was sent to the claimants and to several hundred other recipients with the email addresses visible in CC (Carbon Copy) instead of CCC (Carbon Copy Invisible). In this case, the BDPA didn't assessed the lawfulness ground of the processing of the complainants' email addresses as it was not the subject of the complaint. In addition, two arguments were put forward by the defendant. First, it was a regrettable individual error made by an employee. Second, the email did not contain any personal data (including sensitive data) since the only information disclosed to the recipients was the email addresses of the other recipients. The defendant also indicated that various protection measures had been taken within the FSMA in order to comply as much as possible with the GDPR (e.g. appointing a DPO and organising training courses in data protection for the employees). In the decision, the litigation chamber recalls articles 24.1, 25 and 74 of the GDPR relating to the rights and duties of the controller as well as the latter's accountability. The BDPA found that the defendant had failed to comply with these articles because, as a controller, it had not taken the appropriate technical and organisational measures to ensure and be able to demonstrate that processing at hand was compliant the GDPR. Therefore, the authority decided to issue a reprimand.

RIGHT TO ERASURE – RIGHT TO BE FORGOTTEN

Brussels Court of Appeal, Brussels Markets Court, 19th Chamber A, judgment of 26 October 2022

An appeal was lodged against the decision taken by the BDPA on 17 March 2022 (decision 38/2022 already commented in the previous report).

The appeal concerned a rejected-complaint filed by a lawyer to whom Google had refused dereference in various press articles reporting the lawyer's previous convictions and subsequent disbarment. The BDPA below nevertheless issued a reprimand to Google Belgium for non-compliance with articles 12.1, 12.2 and 17 of the GDPR. Google Belgium and Google LLC (the claimants) are also appealing the BDPA's decision with regard to this reprimand. According to the claimants, the authority violated the provisions of the GDPR in that it found an infringement of the Regulation and issued the related penalty to a local establishment of Google LLC (i.e Google Belgium) whereas it also acknowledged that Google LLC, being the controller, is the one bound to comply with the infringed rules. The claimants also appealed the BDPA's decision for alleged lack of reasoning . In particular, they challenged the fact that the appealed decision was referring to one of the BDPA's decisions (decision no. 37/2020) which has since been annulled by the Market Court. The Market Court followed this argument, considering that the illegality of decision no. 37/2020, to which the BDPA referred in order to impose the sanction against Google Belgium, justified the annulment of this sanction. The Court considers that a "motivation by reference" can only take place if the document referred to exists and is properly motivated. Nevertheless, this was not the case.

Court of Cassation, judgment of 15 June 2022

In this judgment, the Belgian Court of Cassation validates the decision of the Brussels Court of Appeal, after having referred a question to the Constitutional Court for a preliminary ruling on the rehabilitation and deletion of information related to a person's mental state.

Under Belgian law, rehabilitation allows the effects of a criminal conviction to be erased if certain conditions are met. This measure aims to reintegrate the convicted person into society. Following a rehabilitation decision, the mention of the conviction is removed from the criminal record. At the same time, another legal provision (art. 621 of the Criminal Procedure Code) prohibits the rehabilitation of a person who has been interned. In a decision already commented in the previous report, the Constitutional Court was asked by the Belgian Court of Cassation to an-

swer the question of whether this legal provision violates the principles of equality and non-discrimination, in particular because the continued registration of the internment decision in the criminal record reveals the past and the mental state of the person (i.e. an element of his or her private life). The Constitutional Court answered that internment is a measure whose nature and effects cannot be equated with those of a criminal conviction, and that it is justified that rehabilitation cannot be applied to an internment decision. The legal provision is therefore valid. Hence, the Court of Cassation refuses to overturn a judgment of the Brussels Court of Appeal (Indictment Division) which rejected the application for rehabilitation of a person who had been interned, on the grounds that the Belgian legal provision did not allow rehabilitation to be granted to an interned person. The Court of Cassation considered that the court had legally motivated its decision.

DATA PROCESSING OF DATA CONCERNING INDIVIDUAL OFFERING HOUSING SERVICES ON PLATFORMS

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 162/2022 of 16 November 2022

The BDPA ruled on GDPR compliance of surveys sent by the Tourist Office of Flanders (the defendant) to housing intermediaries in order to obtain personal data of housing operators to carry out controls.

The authority decided to investigate a practice of the defendant which consisted in sending request to Airbnb in order to obtain personal data of individuals offering housing services through the platform. The defendant however argued that the data processing was necessary to comply with a legal obligation (art.6.1.c. GDPR). In line with this argument, the litigation chamber noted that article 10 of the Flemish decree of 5 February 2016 on housing grants to the defendant's inspectors the duty to verify compliance with the requirements on touristic housing services. In addition, article 11 of this decree contains three different cases in which personal data can be requested, in a targeted manner, from housing intermediaries such as Airbnb. These cases include, among others, clearly delineated surveys. This was further confirmed in the preparatory works of the decree. Thus, the BDPA considered the data processing as necessary to apply the housing legislation and to comply with the defendant legal obligation. Regarding the data collected from intermediaries (e.g. address of the housing, name and email address of the housing operator), the BDPA also considered it as necessary for the processing. Therefore, the processing was lawful and did not violate data-minimisation principle. In contrast, the BDPA found violations of the transparency principle and the data subjects' rights of information (arts. 5, 12, 13 and 14 GDPR). In this sense, the privacy policy on the defendant's web portal contained outdated and incomplete information (e.g. the privacy policy contained references to the repealed law transposing the data-protection directive and only mentioned the possibility to lodge a complaint before a supervisory body established by a federated entity). Finally, the defendant failed to consult its DPO in due time regarding the processing (violation of arts. 38 and 39 GDPR). Consequently, the authority issued reprimands for these violations.

Constitutional Court, judgment 148/2022 of 17 November 2022

The Constitutional Court was asked to rule on the validity of an Order (i.e. a legislative norm adopted by a federated entity) obliging intermediaries to provide, to the tax administration, data on users offering housing services via their platforms.

Airbnb (the claimant) brought an action for annulment before the Constitutional Court against article 12 of an order of the Brussels-Capital Region of 23 December 2016 on the regional tax on touristic housing. This provision applies to intermediary housing-services providers such as the claimant. The first paragraph creates a duty to provide, on written demand, to the tax administration of the Region data relating to operators offering housing services in the Region through their platforms. If an intermediary fails to provide the data, a fine of 10.000€ can be imposed (second paragraph). According to the claimant, the provision creates, among others, an unjustified interference with the rights to privacy and data protection of the individuals using its platform to offer housing services in the Region. In the decision, the Court recalled that such provision indeed interferes with the right to privacy of the operators and that the Brussels legislator is bound by the guarantees of the GDPR. The Court however considered the interference as reasonably justified. To this extent, the provision aims to achieve legitimate objectives, which are the correct establishment of the regional tax on touristic housing and the verification of the operators' compliance with their tax duties. Fur-

thermore, the data to provide (i.e. name and address of the operator, contact details of the housing establishment, number of nights and establishments operated during the year) are sufficiently delimited. Finally, data transmission is not automatic and tax-administration's officials are bound by professional secrecy. Therefore, the Court upheld the first paragraph. In contrast, the Court decided that the impossibility to diminish the amount of the fine is contrary to the requirement of imposing proportioned punishments (violation of arts. 10, 11 of the Constitution and art.6 of the European convention on human rights). Hence, the Court annulled this paragraph.

RELATIONS BETWEEN INVESTIGATIVE POWERS OF THE TAX ADMINISTRATION AND THE RIGHTS TO PRIVACY AND DATA PROTECTION

Belgian Data Protection Authority (BDPA) (litigation chamber), decision 134/2022 of 15 September 2022

The BDPA had to rule on a complaint filed against the tax administration (SPF Finances) for data-processing operation during tax investigation.

In this case, the defendant collected personal data while visiting various undertakings in which the claimant is involved. Then, the defendant sent to the same undertakings notifications of extension of the investigation which contained data on private trips of the claimant (e.g. locations and costs). According to the claimant, this practice resulted in violations of the GDPR. In its decision, the litigation chamber first recognised that it may sometimes be complicated for a claimant to identify the data controller. In such cases, the BDPA is competent to establish its identity. The authority also confirmed that the defendant determined purposes and means of the processing (by collecting data from undertakings and choosing which data to include in the notifications). Furthermore, the defendant is de jure qualified as data controller by the Belgian act of 3 August 2012 on data processing carried out by SPF Finances. Then, the litigation chamber recalled that data processing done on this basis falls within the scope of the BDPA's competences. In the same time the decision recalls that, in accordance with its "closing with no further action" policy, it is not the authority's priority to intervene in ongoing administrative proceedings. Although the authority is competent to verify the necessity of data processed for a tax investigation (i.e. the public interest task of the defendant) it must show extreme restraint. Therefore, it cannot substitute itself for the tax administration, which has a broad discretionary power to assess which data are necessary to carry out a proper tax investigation and to perform its tasks. Furthermore, tax proceedings – including data-protection issues – can still be subject to the appreciation of a judicial court. For this reason, the BPDA decided to reject the complaint.

Constitutional Court, judgment 162/2022 of 8 December 2022

The Constitutional Court refused to annul a law that imposes inclusion of additional personnel data in an already-existing database called "Point de Contact central" (PCC) managed by the National Bank of Belgium (NBB).

Before the Constitutional Court, two natural persons and a legal person (the claimants) requested the annulment of articles 18 to 22 of the program act of 20 December 2020. The contested provisions created a duty for financial entities (e.g. banks and credit institutions) to provide additional data related to taxpayers in the PCC. The data include the periodic balances of banks and payment accounts as well as the periodic aggregate amount of certain financial contracts. The provisions also allow the tax administration in charge with VAT to access the data where evidence of tax fraud exists (as it was already the case in the field of income taxation). The claimants alleged that such practices constituted an unjustified interference with the right to privacy. However, the Court rejecyed the complaint on several grounds. First, according to the Court, all the purposes aimed by the PCC database must be considered while assessing the validity of the contested provisions. To that extent, the mandatory inclusions of the additional data aims to fight tax evasion but also helps judicial authorities and intelligence services to contrast terrorism and serious crime. Second, subject to a prior opinion of the BDPA, any person entitled to receive data from the PCC must be explicitly authorised by the legislator to request them in order to perform a task in the public interest enshrined by law. Third, in the field of taxation, the data can only be requested where there is evidence of tax evasion. Fourth, citizens can request to the NBB the identity of any person who has received his or her data in the six months prior to the request. Finally, the Court also notices that the persons entitled to receive the data must ensure confidentiality and cannot process data for unlawful purposes.

Constitutional Court, judgment 103/2022 of 15 September 2022

An action for annulment is brought before the Constitutional Court against the Belgian act of 20 December 2019 transposing the EU directive 2018/822 of 25 May 2018 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements (Directive 2018/22).

In this case, claimants - including the national bar associations and the institute of chartered accountants - requested the annulment of the contested act transposing the EU directive 2018/822. This act modifies several Belgian tax codes (i.e. income tax code, code of registration and mortgage fees, inheritance tax code and code of miscellaneous duties and taxes). In substance it creates a duty to provide the tax administration with data relating to cross-border arrangements that indicate the risk of tax avoidance. Information on these arrangements is then automatically shared with other member states. Such duty applied to intermediaries (i.e. any person which, among others, designs or markets reportable arrangement, or offers advices in this regard). Where intermediaries are subject to professional secrecy, the duty of declaration applies to other intermediaries and ultimately to the taxpayer. For marketable arrangements (i.e. arrangement that can be implemented without substantial customisation) intermediaries must also provide, every three months, a report containing updates such as name of the concerned taxpayers. In such case, they cannot invoke professional secrecy. Therefore, the claimants argued, among many claims, that this mechanism infringes upon attorney-client privilege as well as the duty of confidentiality applying to other professions. Regarding this claim, the Court recalled that attorney-client privilege is an essential component of the rights to a fair trial and privacy, which also apply to legal advice provided outside legal proceedings. The Court acknowledged however that privilege does not extend to information otherwise disclosed, such as the ones provided in periodic reporting. Hence, the Court considered that the absolute privilege is not proportionate since lawyers can still provide information to be declared to the taxpayer (especially as marketable arrangements do not need substantial customisation). Likewise, absolute priviledge for other professions is also not proportionate. Thus, the Court annulled the provisions of the codes as modified. Among others, the claimants also argued that the mechanism of mandatory declaration was contrary to rights to privacy and data protection. Regarding this claim, the decision highlights that a duty to disclose also lawful, genuine and not abusive arrangements is created by the Directive. Therefore, the Court referred a question to the EU Court of Justice for a preliminary ruling. In particular, it questions whether the reporting obligation created by the Directive does not constitute a disproportionate interference with the rights to privacy and data protection.

PERSONAL DATA PROCESSED FOR EVIDENTIAL PURPOSES

Corporate Court of Namur (2nd chamber), order of 26 July 2022 available in Revue de jurisprudence de Liège, Mons et Bruxelles (J.L.M.B.), 2023, no 1, p.7

The Court considers that consulting and copying an agenda, in order to use it as evidence to support a legal claim, is a processing of personal data within the meaning of the GDPR.

Under Belgian law, in civil disputes, the use of unlawfully-obtained evidences cannot be dismissed. This principle applies unless (1) the law provides otherwise, (2) the obtaining of the evidence would undermine its reliability or (3) the obtaining of the evidence compromises the right to a fair trial. In the case at hand, the Court had to rule on a dispute concerning an alleged breach of a non-competition clause in a business-transfer agreement. In order to prove the breach of the clause the claimant consulted the defendant's agenda. On this occasion, he discovered, the presence of suspicious appointments and events. According to the Court, the consultation and making a copy of a diary must be considered as "processing" within the meaning of the GDPR. In order to ensure compliance with the GDPR, the Court considers that in the case of personal data collected in the context of the preparation of a file to support a legal claim (i.e. data processed for evidentiary purposes) it is necessary to verify, (1) whether the data have been processed fairly and lawfully, (2) whether the purposes are specified, explicit and legitimate and (3) whether the data are relevant, adequate and strictly necessary. According to the Court, the consultation of the agenda for a period not covered by the non-competition clause does not constitute the pursuit of a legitimate interest on the part of the applicant. Hence, the data were not processed in accordance with article 5 of the GDPR. However, as the copy of the consulted

agenda was disclosed to the other party, the rights of defence were respected and there was no breach of the right to a fair trial. The Court also considers that the evidence of contacts with customers (which is supported by the agenda) is a useful and necessary element for the resolution of the dispute. Therefore, the Court does not reject the document and declares it admissible evidence.

PERSONAL DATA PROCESSED IN THE FIELD OF EDUCATION

Belgian Data Protection Authority (BDPA) (Litigation chamber), decision 175/2022 of 28 November 2022

The BDPA had to rule on complaints filed against an educational institute for social promotion (the first defendant) and its education authority (the second defendant).

The BDPA received two complaints filed by a former student of the first defendant against the first defendant (not possessing the legal personality) and the second defendant (having the legal personality). The first complaint was directed against the sending of a group email to several students with the email addresses of all recipients visible. The second concerned the public display of students' results with the mention of their names and date of birth. The BDPA determined the capacity of each of the defendants in order to determine who was accountable for the processing. To that extent, the litigation chamber recalled that an entity such as the first defendant which has no legal personality (e.g. a de facto association) can be qualified as data controller. Considering the factual elements of the case, the second defendant was however the data controller. Therefore, the authority decided to close the complaint against the first defendant. With regard to the two complaints, the BDPA analysed whether the sending of the email to all students was based on a specific purpose and was relying on a lawfulness ground (articles 5.1.a. and 6 RGPD). In the present case, given the description of the limited purposes for which the email address was collected at registration, the further processing (i.e. to allow communication in the framework of a course) cannot be qualified as permissible. Nor did the defendant rely on a permissible lawfulness basis for the processing at issue. It also considers that the principles of transparency and minimisation have not been respected. In particular, the decision highlights that public display of students' results with name and date of birth instead of results and matricula infringes the GDPR. The BDPA concluded that Articles 5.1.a., 6 and 12.1. GDPR were violated. It therefore issued reprimands.

FRANCE

edited by
Mehdi KIMRI, Ph.D. Candidate in Public Law, University of Côte-d'Azur
Julien MONGROLE, Ph.D. Candidate in Public Law, University of Limoges
Raphaël MOURERE, Ph.D. Candidate in Private Law, University of Côte-d'Azur
Quentin RICORDEL, Ph.D. Candidate in Public Law, University of Limoges
Guillaume TOURRES, Ph.D. Candidate in Public Law, University Paris 1 Panthéon Sorbonne

DIGITIZATION OF ADMINISTRATIVE PROCEDURES

Investigation by the Defender of Rights, 26 January 2022, on the availability of public service telephone platforms

On 26 January 2023, the Defender of Rights and the National Consumer Institute published the results of a joint survey on the availability and quality of the telephone platforms of four public services.

In France, the dematerialization process initiated by the Government through the "Public Action 2022" Plan is the subject of significant debate, particularly as regards the effectiveness of access to people's rights. The massive use of tele-services and the concomitant closure of reception areas to the public deprive people who do not have adequate computer equipment or knowledge of regular access to public services. The impossibility of accessing public services online leads to situations of non-use of rights and aggravates the financial or social precariousness of certain users. Several reports by the Defender of Rights have reported on these issues, as is the case with the 2019 report "Dematerialization and inequalities of access to public services" (www.defenseurdesdroits.fr/fr/rapports /2019/01 /dematerialisation-et-inegalites-dacces-aux-services-publics), supplemented in 2022 by a second report "Dematerialization of public services: three years later where are we? (www.defenseurdesdroits.fr/fr/rapports/2022/02/ rapport-dematerialisation-des-services-publics-trois-ans-apres-ou-en-est-on).

Faced with the gradual closure of public-

service counters, the use of administrative telephone platforms is essential in order to maintain several methods of access to public service. With a view to testing the accessibility of public services by telephone, the Defender of Rights and the National Consumer Institute conducted a survey on the availability and quality of public-service telephone platforms. This survey follows a first study published in 2016 “Telephone reception and dematerialization of public services. The results of a mystery investigation”.

This new study focused on the telephone platforms of four French public services. Namely: the Family Allowance Fund (CAF), Pôle Emploi, the Health Insurance and Pension Insurance (CARSAT). It aimed to determine “whether it was easy to reach these organizations by telephone and to collect useful information to benefit from a benefit”. To do this, several “caller profiles” were used to contact the administrations concerned and obtain information. Among these profiles, it is possible to mention: a person with internet access, a person who does not have internet access, a person who does not have a good command of French language, and finally an elderly person with internet access.

The conclusions of this investigation are divided. If the “friendliness” of the interlocutors has been noticed, the rate of satisfactory answers never exceeds 60% and the waiting time before obtaining an interlocutor is generally more than 9 minutes. In other words, “on the 1,500 calls made as part of the survey, 40% were unsuccessful”. In addition, the Defender of Rights denounces the systematic referrals to the teleservices of the administrations concerned, despite the presence among the profile of callers of a "person without internet". A questionable practice more generally, since according to the National Institute of Statistics and Economic Studies (INSEE), nearly 17% of the French population suffer from illiteracy, and 7% do not have internet access at home.

Decree no 2023-64 of 3 February 2023 creating a processing of personal data called "NATALI"

The decree of 3 February 2023 aims to create a processing of personal data called NATALI. This teleservice is set up to allow users to carry out electronically the steps necessary to obtain French citizenship, to francize surnames and first names and to authorize the loss of French citizenship.

Since the beginning of 2021, the procedures relating to the applications and renewals of residence permits have been increasingly dematerialized. Several regulatory texts have intervened in this direction, this is particularly the case of decree n ° 2021-313 of 24 March 2021, the order of 27 April 2021 and the order of 19 May 2021. These various texts, which aimed to generalize the use of a teleservice for applications for certain residence permits were challenged before the Council of State, which ruled on the occasion of a judgment of 3 June 2022 no. 452798. The administrative judges considered that the obligation imposed on users to use a teleservice is not illegal, but that it must be accompanied by additional measures so as not to exclude people experiencing some difficulty with the digital tool.

It is clear that despite these decisions, the Government's objectives are tending towards an increasing generalization of teleservices in the context of applications for residence permits. The decree of 3 February 2023 authorizes the Minister of the Interior to implement the processing of personal data "NATALI". These teleservices have several purposes (article 1):

First, to allow foreigners to complete the procedures for acquiring nationality online by reason of marriage, ascendant status or status of brother or sister of French nationality. The procedures for acquiring French nationality by decision of the public authority and for reintegration into nationality are also covered; francization of surnames and first names; and authorization to lose the French nationality.

Secondly, to allow the central and local services of the ministry, as well as the diplomatic and consular authorities to ensure the processing of requests, but also that of administrative and contentious appeals that may occur.

Third, to allow users or their representative to exercise administrative recourse against decisions concerning them.

The personal data processed in the "NATALI" automated processing (article 2) are mentioned in the first appendix to the decree, and are only accessible within the "limit of the need to know" by strictly identified agents, individually designated and specially authorized (Article 3). These include agents responsible for applying the regulations relating to the acquisition, withdrawal, forfeiture and loss of French citizenship and coming under the central services of the Ministry of the Interior. and the Ministry of Foreign Affairs, also agents of the prefectures and sub-prefectures and agents of the diplomatic or consular services. With regard to the recipients of these personal data, this decree establishes a list in its article 4, distinguishing them ac-

cording to the type of data concerned.

The retention periods for personal data are mentioned in article 5. For data corresponding to the identifier, the password, as well as those resulting from communications between the administration and the person concerned, identified benefiting from a user space and those concerning the identifier of the agent, the legal representative, the lawyer or the spouse, the retention period is 3 years from the final decision of the administration. For all other data mentioned in the appendix, the retention period is 3 years from the date of publication in the Official Journal of the decree of naturalization, reintegration into French nationality or release from ties of allegiance, or from the date of registration of the declaration or francization decree. Article 5 provides for variable retention periods in the event of refusal and a decision to classify without further action.

Finally, Articles 6 and 7 provide the procedures for exercising the rights relating to the protection of personal data.

PROTECTION OF PERSONAL DATA

Commission nationale de l'informatique et des libertés (CNIL), Deliberation 2022-118 of 8 December 2022

The CNIL had the opportunity to rule on 8 December 2022 on the bill relating to the 2024 Olympic and Paralympic Games, presented by the Government to the Council of Ministers on 22 December 2022.

The bill relating to the 2024 Olympic and Paralympic Games provides for several derogations from ordinary law in order to ensure the proper organization of the event. Several provisions of the bill present strong stakes in terms of personal-data protection. This is particularly the case:

- Authorizing the examination of the genetic characteristics or the comparison of the athlete's genetic fingerprints for the purposes of the fight against doping (article 4);
- Compliance of the Internal Security Code (CSI) with the GDPR and the law of January 6, 1978 (article 5);
- The use of augmented cameras (article 6);
- The extension of the video-protection images that the agents of the internal services of the SNCF and the RATP can view when they are assigned within the information and command rooms coming under the State (article 7);
- The extension of the screening procedure provided for in article L211-11-1 of the CSI to fan-zones and participants in major events (article 9);
- The possibility of setting up body scanners at the entrance to sports arenas (article 10).

It is on all of these articles that the CNIL had to rule in the context of the deliberation of 8 December 2022. Particular attention will be paid to articles 4,5,6,7 and 10 of the bill.

Firstly, concerning the examination of genetic characteristics in the context of anti-doping tests. Article 4 of the bill aims to ensure compliance with domestic law with the provisions of the World Anti-Doping Code. To do this, the article provides for several derogations from the provisions of the Civil Code for the purposes contrasting doping. The CNIL, while acknowledging the need to adapt domestic laws, stresses that "these would be particularly intrusive tests, which significantly derogate from the principles currently governing the analysis of genetics in the Civil Code". In addition, the regulator urges the Government to explain the conditions for informing and obtaining the consent of the athlete subject to these analyses.

Secondly, on bringing the Internal Security Code (CSI) into compliance with the General Data Protection Regulation and the Data Protection Act of 6 January 1978. Indeed, the bill intends to bring the CSI, particularly Articles L.251-1 and L.255-1, within the provisions of the GDPR and the French Data-Protection Law regarding the protection of personal data. While acknowledging the benefit of bringing the video protection regime provided for by the CSI into compliance, the CNIL denounces "the choice to modify the existing provisions as a minimum [...]" and calls for a "more global" reform of the regime relating to the "processing of images in spaces open to the public […]" as well as "general" compliance with the CSI.

Third, on the experimentation of "augmented" cameras. Article 6 of the bill aims to experiment with "algorithmic processing of automated analysis of images from video-protection devices and cameras installed on aircraft in order to detect and report events in real time.". These systems based on artificial-intelligence systems are intended to "ensure the security of sporting, recreational or cultural events which, by their size or their circumstances, are particularly exposed to the risk of acts of terrorism or risk of serious harm to the safety of persons". As such, any use of augmented cameras for other purposes is ruled out. The regulator recognizes the legitimacy of these objectives, but recalls "that the de-

ployment, even experimental, of these devices of augmented cameras is a turning point which will contribute to defining the role which will be entrusted in our society to these technologies, and more generally to "artificial intelligence". In addition, it specifies that the guarantees provided for by the bill are consistent with the recommendations formulated in its position paper on the deployment of augmented cameras in public spaces, published in July 2022 (www.cnil.fr/fr/deploiement-de-cameras-augmentees-dans-les-espaces-publics-la-cnil-publie-sa-position). To know:

- "An experimental deployment;
- Limited in time and space;
- For certain specific purposes and corresponding to serious risks for people;
- The absence of biometric data processing;
- The lack of reconciliation with other files;
- The absence of automatic decision-making: the algorithms are only used to signal potentially problematic situations to people who then carry out a human analysis".

Fourthly, with regard to the extension of the video surveillance images that the agents of the internal services of the SNCF and the RATP can view. Article 7 of the bill aims to extend the spectrum of video-protection images that can be viewed by agents of the internal security services of SNCF and RATP, the two main transport players in the Ile-de-France region. This extension aims to ensure "better management of the flow of supporters going to sites served by the means of transport of the two operators, or leaving them at the end of the sporting event" and to allow "the improvement of the communication between the different people involved in the flow of people in the context of major sporting events". For the CNIL, the possibility offered to SNCF and RATP agents to access more images should not lead to an extension of their competence at the same time. These remain limited to missions of prevention and safety of persons and property. Furthermore, the CNIL suggests that the bill be clarified so as not to imply that access to the images can be done without restriction.

Lately, on the possibility of setting up body scanners at the entrance to sports arenas. The implementation of body scanners proposed by article 10 aims to streamline and secure people's access to areas determined by decree. For the CNIL, the various conditions defined by the bill (consent of the data subject, respect for anonymity, system blurring the visualization of the face, prohibition of the recording and storage of images, etc.) makes it possible to reduce violations "to the privacy and intimacy of the persons concerned". On the other hand, it recalls that these devices constitute processing of personal data within the meaning of the Communication from the Commission to the European Parliament and the Council on the use of security scanners at airports in the European Union of 15 June 2010 (COM/2010/0311 final) and that they remain subject to the relevant regulations. In addition, the CNIL calls for particular vigilance with regard to the procedures for obtaining consent and informing the persons concerned.

Court of Cassation, 1st Civil Chamber, 5 January 2023, No. 22-40.017

In a decision dated 5 January 2023, the Court of Cassation refused to transmit the priority question of constitutionality raised in the context of a dispute with the Autorité de Régulation de la Communication Audiovisuelle et Numérique (French regulatory authority for audiovisual and digital communication), concerning measures to block access to pornographic sites in order to protect young people.

In this case, a number of internet service providers were challenged in relation to access by minors to websites containing pornographic content. This access is open to any user who simply declares that he or she is not a minor. However, article 227-24 of the Penal Code punishes the offence of manufacturing, distributing or trading a pornographic message when this message is likely to be seen or perceived by a minor. Moreover, the third paragraph of the article specifies that the offence is constituted "even if the access of a minor to the messages [...] results from a simple declaration by the minor indicating that he or she is at least eighteen years of age".

The Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) is the independent administrative authority empowered to control the existence of such access to pornographic content. On the basis of article 23 of the law of 30 July 2020 no 2020-936 aiming at protecting victims of domestic violence, the president of ARCOM has the power to give formal notice to any person whose activity is to publish a service of communication to the public on line, so that the latter takes all the necessary measures to prevent the access of minors to pornographic content. In case of non-fulfilment of the injunction, the president can then refer the matter to the judicial court in order to close access to the content according to the accelerated procedure on the merits; which in this case has

been done. At this stage of the proceedings, one of the companies involved in the case raised a priority question of constitutionality concerning the provisions of article 23 of law no 2020-936.

Although the provision in question defines, at first glance, the criminal offence as well as the conduct that may give rise to a sanction in sufficiently-clear and precise terms, the character of necessity, adaptation and proportionality to the objective of protecting minors could raise questions. Indeed, by deeming insufficient a control by declaration, article 23 of the law no 2020-936 imposes on internet-access providers as well as on publishers of pornographic content sites, and more generally of content unsuitable for minors, to implement a stricter control. What about the modalities of such a stricter control, which presents practical and economic difficulties? The Paris Court of Justice has thus transmitted the priority question of constitutionality to the Court of Cassation, which has examined it. Therefore, article 23-4 of the organic law no 2009-1523 of December 10, 2009 on the application of article 61-1 of the French Constitution provides the conditions for the examination of a priority question of constitutionality by the French Constitutional Council. The questioned provision must be at issue in the pending litigation, it must not have already been declared in conformity with the French Constitution by the Constitutional Council and, finally, the question must be new or present a serious character. The Court of Cassation noted that if the first two conditions were met, the question was not new in that the provision had already been applied by the Constitutional Council. In addition, the court noted that "the infringement of the freedom of expression, by requiring the use of a device to verify the age of the person accessing pornographic content, other than a simple declaration, is necessary, appropriate and proportionate to the objective of protecting minors. The measures to control the age of users will thus have to be reinforced, requiring operators to bear the cost and responsibility of a new processing in the sense of personal-data protection law.

SUMMARY INJUNCTION AND PROSECUTION DISTINCTION

Paris judicial court, summary order 21 December 2022, Noctis Event et M. X. / Wikimedia Foundation Inc

In a summary order dated 21 December 2022, issued on the basis of article 145 of the French Code of Civil Procedure, the Paris judicial court distinguished between a judicial-information measure and a protective measure ordered in summary proceedings. The court held that the communication of identification data of a user who created a Wikipedia page under the cover of a pseudonym constitutes an investigative measure legally admissible by the judicial judge, independently of the principle according to which only the public prosecutor has the right to prosecute.

In this case, the company Noctis Event and its director were targeted in a Wikipedia page created by an unknown person acting under a pseudonym. The elements gathered in the page showed the particular malice of the author against the designated company and its manager: "he cheats at his baccalaureate, with earphones and a cheat sheet", "he is a cousin of the anti-Semitic director Pierre Ramelot", "he is a cousin of the pedophile writer Henry de Montherlant". The company and its director then asked the Wikimedia company to communicate the identification data of the author of the litigious page. Let us recall that article L.34-1 of the Code of the posts and electronic communications stipulates that the operators of electronic communications are held to preserve, for the needs "in particular of the penal procedures" - but not only, the information relating to the civil identity of the user until the expiration of a 5-year deadline as from the end of validity of its contract, and the other information provided by the user at the time of the creation of an account, until the expiration of a one-year deadline as from the closing of the account. However, Wikimedia refused to make the disclosure despite being ordered to do so by a motion order. Wikimedia was consequently summoned in summary proceedings by the company Noctis Event to comply.

On the basis of article 145 of the French Code of Civil Procedure, the court examined the "legitimate reason" put forward by the plaintiff company. The existence of this legitimate reason is a prerequisite for any investigative measure aimed at preserving or establishing, before any trial, evidence of facts on which the solution of a dispute could depend. Exercising its discretion as a judge of the merits, the court concluded that the filing of a lawsuit for denigration or on the basis of the criminal offence of cyberstalking did constitute a legitimate reason. The court notes that the exercise of such an action is not obviously doomed to failure in this case; the identification of the author of the page being however essential to its success. Thus, the court judged that the communication of the identification data

was necessary for the exercise of the right to evidence and proportionate to the antinomic interests at issue.

The judgment has the advantage of distinguishing between the taking of a precautionary measure ordered by the judge and an investigative measure taken in the context of a judicial investigation, which is conditional on the exercise of the public prosecutor's action. Article 80 of the French Code of Criminal Procedure stipulates that a judicial investigation can only be opened upon the request of the public prosecutor. The judicial investigation must make it possible to determine the existence of an offence and to identify the perpetrators. However, the Paris judicial court specifies that "the mere fact that the public prosecutor has the opportunity to prosecute, as the Wikimedia Foundation Inc. maintains, cannot suffice to render the requested investigative measure, which is aimed at identifying the author of these acts, unlawful. The judge can thus order communication measures relating to facts likely to be subject to criminal sanctions before the public prosecution is initiated, insofar as the evidence concerned is necessary for the exercise of a civil liability action; in this case for denigration. Indeed, the interest of this evidence cannot be limited to the framework of the investigation carried out during a judicial investigation in anticipation of a criminal trial.

COUNTERFEITING AND RESPONSE TO A PUBLIC INVITATION TO TENDER

Court of Cassation, 1st Civil Chamber, 5 October 2022, No. 21-15.386, Entr'ouvert / Orange and Orange Business Services

In a decision dated 5 October 2022, the First Civil Chamber of the Court of Cassation clarifies that the owner of a copyright on a software that he has licensed is entitled to bring an action for infringement against the licensee who has used said software to respond to a public tender, in violation of the stipulations of the license agreement.

In this case, the company Entr'Ouvert conceived a software named “Lasso” allowing the installation of a unique authentication system. It diffused this software under free license. In order to answer the call for tender of the French State for the realization of the portal "My public service", the company Orange had developed a software platform for management of identities and means of interface for service providers. But this platform integrated the Lasso software. The company Entr'Ouvert then sued the company Orange for copyright infringement and economic parasitism, arguing that this use of its software was not in conformity with the stipulations of the free-license contract. In a decision dated March 19, 2021, the Paris Court of Appeal awarded Entr'Ouvert the sum of 150,000 euros in damages for economic parasitism exercised by the company Orange. The sum was far from the 500 000 euros of damages initially requested by the company, for lack of sufficient evidence of the extent of the economic damage suffered, according to the assessment of the judges of the court. In addition, the judges of appeal declared the copyright-infringement action of the company Entr'ouvert inadmissible. Entr'ouvert then appealed against this decision.

Pursuant to Article L. 335-3, paragraph 2, of the French Intellectual Property Code, Articles 7 and 13 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, and Article 1 of Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, the Court of Cassation found that in the case of copyright-infringement on software, the owner does not benefit from the guarantees provided for in Articles 7 and 13 of Directive 2004/48/EC of the European Parliament and of the Council of April 29, 2004, when he acts on the basis of contractual liability under ordinary law. Consequently, the judges of cassation specify that the owner can act in infringement. Their reasoning takes into account the interpretation of the judges of the Court of Justice of the European Union of the aforementioned European directives.

The judges of the Union had indeed specified in a judgment of December 18, 2019, C-666/18, that "the infringement of a clause in a computer-program licensing agreement, relating to the intellectual property rights of the holder of the copyright in that program, falls within the scope of infringement of intellectual property rights, within the meaning of Directive 2004/48, and that, consequently, that holder must be able to benefit from the safeguards provided for in that directive, irrespective of the system of liability applicable under national law. However, in this case, the judges of appeal did not take into account elements other than economic factors, such as the moral prejudice caused to the right holder by the infringement. Furthermore, the compensation awarded to Entr'Ouvert did not include, as an alternative, a lump sum of damages, based on elements such as, at least, the amount

of the royalties or fees that would have been due if the infringer had requested permission to use the intellectual-property in question. The company Entr'Ouvert could not indeed profit from the guarantees offered by directive 2004/48 within the framework of an action in contractual civil liability. In this action for non-performance of the contract of license, the amount of the damages cannot exceed what is foreseeable at the conclusion of the contract or what the parts envisaged conventionally; according to former article 1147 of the French Civil code in its version applicable to the case (current article 1231-1 of the French Civil code). The re-exploitation in the response to a public contract in contravention of the stipulations of a software-license agreement, is thus likely to expose the candidate to the payment of damages for copyright infringement.

ITALY

edited by
Alessia PALLADINO, Ph.D. in Administrative Law, University of Naples Suor Orsola Benincasa

EXCLUSION OF THE ECONOMIC OPERATOR IN CASE OF NEGLIGENCE IN E -PROCUREMEN PROCEDURES

Regional Administrative Court of Umbria, decision 761/2022 of 27 October 2022.

In this ruling the Regional Administrative Court of Umbria rules that the competitor who tried to upload the tender documents on the Me.pa telematic platform within the fixed time, but could not finalize the sending and does not take a diligent actions by immediately reporting the malfunctioning and asking for remedies, shall be excluded from such tender procedure.

The Regional Administrative Court of Umbria, Perugia, clarifies the specific duties of fairness, accountability and diligence upon to the economic competitor who decides to join a public tender and tries to upload the tender documents on the telematic platform.

The dispute arose from the action brought before the Regional Administrative Court of Umbria, by an economic operator who contested the exclusion from a simplified-negotiated procedure on the Me.pa platform.

Due to a technical malfunctioning, the operator alleged the impossibility of entering the fields reserved for the technical and economic documentation.

Consequently, they decided to upload the technical and economic offer in the field relating to the administrative documentation. Therefore, to ensure the respect of secrecy and impartiality, the offers were distinguished in three different files.

In its judgment of 27 October 2022 no 761, the Regional Administrative Court of Umbria rules that whenever the tender procedure is characterised by a clear separation between the evaluation phase of the technical tender and the evaluation phase of the economic offer, the principle of unfairness means that until the evaluation of the technical elements is completed, the economic offer must be kept secret, to avoid any possible influence on the evaluation of the technical elements. In particular, the mere possibility of knowing the extent of the economic offer, before the technical one, is prone to jeopardize the guarantee of impartiality of the assessment.

Therefore, the Court recalls long –-lasting opinions and previous judgments (Regional Administrative Court of Lazio, Rome, sect. II, decision of 16 December 2021, no 13081), which underline a renewed-accountability attitude addressed to the economic operator.

The Court argues that widespread e-procurement calls for particular care and diligence in uploading the documents, with the consequent impossibility of attributing to the Contracting Authority any type of anomaly in the mechanism of re-registration.

Beside all, in case of proven technical malfunctioning of the platform, which avoids the transmission of the tender documents, the economic operator must take diligent steps by immediately reporting it to the Contracting Authority, and asking for remedies provided by Article 79, paragraph 5-bis, of the legislative decree no 50/2016.

In this regard, the operator must be diligent, by asking for (i) an extension or (ii) a suspension of the deadline, as well as (iii) the opening a ticket for technical support. On the contrary, the Court underlines that in the case at issue the economic operator just uploaded the tender documents together, providing a mere screenshot, that it found unsuitable to prove the platform malfunction.

As a consequence, the Court states that the exclusion was legitimate.

The analysis of the judgment of the Italian Regional Court of Umbria allows to conclude that, in the event of a software malfunctioning, the economic operators which have started uploading the documents and discover the failure,

shall act diligently by immediately reporting the malfunctioning to the contracting authority, and asking for remedies to complete their submission within a reasonable time.

In this regard, the decision of the Administrative Regional Court of Umbria confirms the legal precedents, which suggest a renewed morphology of economic operator's duties in the e–procurement sector.

PROOF OF PUBLICATION ON A WEBSITE THROUGH ITS CACHE

Council of State, Section V, decision no 8123/2022 of 21 September 2022.

The Council of State rules that the allegation of the Google cache, referred to the Contracting Authority institutional website, is eligible to prove the publication of the contracting award notice, as well as to provide the date of its publication.

The decision of the Council of State provides an innovative overview towards the usage of technology to prove the publication dynamics occurred in the Contracting-Authority institutional website.

In particular, it offers the chance to reflect upon the scope of the Google cache.

The appeal arose from the dispute, decided by the Regional Administrative Court of Naples with the decision of the 31 August 2021, no 5660.

The appellant, ranked second at the end of the tender, with a total score of 69.09 points (having obtained 66.38 points for the technical tender and 2.71 for the economic tender, corresponding to a 4.25% discount), against the winner who scored 79,17 points (in details, 69,17 points for the technical offer and 10 for the economic offer, with a decrease of 58%), has appealed all the acts of the tender, as well as the contracting-award notice.

Thus, at a first glance, the defendant claims for the inadmissibility of the action, arguing that it has been proposed late, out of the legal terms: in details, they state that the contracting-award notice was published on 19th January 2021, whereas the company notified the application more than three months later, on 21st April 2021 and filed it on 5th May 2021.

The Council of State preliminarily rejects the exception of inadmissibility for the lateness, proposed by the defendant.

In this regard, the Council underlines that the appellant company, while contesting that the tender-award notice was published on 19th January 2021, has proven that this notice actually appeared on the web no earlier than 2nd May 2021.

This statement has been confirmed by evidence of the cache registered from the portal www.google.it.

As a matter of fact, caching constitutes a process that allows to temporarily store copies of files, images, as well as web pages, to reduce loading time when a user visits a website.

Thus, the Contracting Authority's website page archived by the Google cache has revealed that the last publication on that website occurred on May 2nd 2021, at 6.53 am.

On this ground, the Council considers the appeal admissible.

PORTUGAL

edited by

Luís MANUEL PICA, Ph.D. in Public Law at the University of Minho (Portugal), invited Assistant Professor 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 PROTECTION OF PERSONAL DATA IN THE PUBLIC ADMINISTRATION

Deliberation no 1040/2022, of 2 November 2022 of the National Commission for Data Protection of Portugal (Comissão Nacional de Proteção de Dados de Portugal)

The national body responsible for protecting personal data has decided to condemn a public-administration body for failure to comply with the General Data Protection Regulation.

The National Commission for Data Protection (CNPD), as the Portuguese administrative agency responsible for supervising and enforcing compliance with the provisions relating to the protection of personal data, decided in deliberation nº. 1040/2022, of 2 November 2022, to impose a fine of EUR 170,000.00 on the municipality of Setúbal for breach of i) the principle of confidentiality (art. 5, paragraph 1(f) of the General Data Protection Regulation), ii) the principle of limitation of the right to access and rectifica-

tion of personal data (Article 5, paragraph 1(f) of the General Data Protection Regulation), of (iv) the principle of storage limitation (Article 5, paragraph 1(e) of the General Data Protection Regulation), and of (iv) the principle of transparency (Article 12 of the General Data Protection Regulation) and of the obligation to appoint a data-protection officer (Article 37 of the General Data Protection Regulation), particularly about the processing of personal data of Ukrainian refugees.

In the context of a procedure to support Ukrainian refugees creating a municipal-support line for refugees and the subsequent creation of a personal database of the same, it was decided that the personal data of the beneficiaries would be collected, without providing the necessary and mandatory information at the time of collection, as well as the context in which the collection was carried out, the duration or a reasonable period of time for its storage, and this database would be accessible by third parties without any protection mechanisms that sought to protect personal data. On the other hand, it was verified that there was no mandatory designation of a Data Protection Officer, being Setúbal City Council a municipal body, it was legally obliged to designate a person responsible for the protection of personal data.

In these terms, Setúbal Municipality was condemned of four offences of a misdemeanor nature.

THE PRACTICE OF PROCEDURAL ACTS IN THE ADMINISTRATIVE COURTS AND THE MANDATORY USE OF ELECTRONIC FORMAT

Judgment of the Central Administrative Court of the South of 6 October 2022

The administrative court decided that since the administrative process is exclusively electronic, the information contained in the forms must be duly filled out to avoid discrepancies with the attached files, otherwise only the content of the initial form will be considered.

According to the provisions of article 24 of the Procedural Code of the Administrative Courts, the proceedings before the administrative courts are electronic, and the procedural acts submitted in writing by the parties shall be presented in court by electronic means, by the respective representatives in the computer system of support to the activity of the administrative and fiscal courts (called SITAF), under the terms defined in Ministerial Order nº. 380/2017, of 19 December;

The practice of procedural acts is carried out by filling out the forms made available in the SITAF to which are attached, namely, files with the material content of the procedural document.

Where the forms contain fields for specific information, they should be filled in accordingly, even if such information is included in the attached file. Where there is a discrepancy between the information contained in the form and the file attached to it, submitted, and which is not corrected at the request of the interested party, in the general terms, or raised automatically, the information in the former shall prevail, even if the respective fields are not filled in.

Detecting the discrepancy in the information regarding the witnesses, the registry in compliance with the provisions of the reproduced paragraph 4 of Article 6 of Ordinance Nº. 380/2017, should notify the applicant to proceed, within 10 days, with the completion of the respective form made available in the computer system of support to the activity of administrative and tax courts, under penalty of considering only the content of the initial form.

Determination that has implicit the existence of two forms: the initial one not filled in or wrongly filled in the field concerning the witnesses, given the content of the evidentiary request in the attached defense - which were submitted in the SITAF and, therefore, are unsusceptible, in themselves, of edition or alteration -; and the one to be filled in, following notification to this effect, to put an end to the divergence of information on this matter - consisting of a request form which will follow a similar process to that used for registering the initial petition or the defense, allowing the representative to insert/add or edit, by substitution, parties, such as witnesses, registered (or not) in the SITAF in previous forms and attached files.

DUTY OF CONFIDENTIALITY ON DATA CONTAINED IN PROPERTY TAX RECORDS.

Ruling of the Supreme Administrative Court, 9 November 2022, Case no 0718/22.7BELRA

In this judgement, the Portuguese Supreme Administrative Court considered that information such as the tax-identification number and tax domicile of the owner of a certain building, contained in the property-tax records, constitute data subject to tax secrecy, and therefore can only be disclosed in the strict circumstances foreseen in Article 64 of the General Tax Law.

The property-tax records, kept by the tax au-

thorities (Tax and Customs Authority) for the purpose of taxation of real-estate assets, contain, namely, the characterization of the properties, the location and their taxable value, as well as the identity of the owners. This means those services receive daily requests for information (on the identity and address of the owner(s) of certain properties) from third parties (potential purchasers, owners of adjoining properties, lawyers, solicitors, etc.), with the disclosure of such data being refused on the grounds that they relate to and reveal the tax situation of the taxpayers.

In the case at issue, the court considered that tax secrecy may be defined as a data-protection regime, which covers not only the privacy of tax data themselves (those that express the taxpayer's tax situation - e.g., data relating to the valuation of the property or to tax exemptions), but also the taxpayers' personal data (data of a personal nature obtained in the exercise of or because of tax functions, that is, in the context of tax procedures or actions - such as addresses and tax-identification numbers). It also established that, although property-tax records fall within the concept of "administrative document", and a right of free access applies to these documents (article 5 of the Access to Administrative Documents Act - Law no. 26/2016, of 22 August), since they contain personal data, this right cannot prevail over the protection constitutionally-granted to the privacy of private life, so it will be necessary to invoke a direct, personal, legitimate and constitutionally protected interest that is sufficiently-relevant interest, justifying access to the information (being that the claim that there is a need to contact the owner of the land, or to know if they belongs to the public domain does not fulfill such requirements). Tax secrecy is maintained even if such data are or not freely accessible through other legal and institutional channels (e.g. land registry).

ACCESS TO ADMINISTRATIVE DOCUMENTS CONTAINING COMMERCIAL, INDUSTRIAL OR COMPANY SECRETS

Ruling of the Southern Administrative Central Court, 8 September 2022, Case no 399/22.8BESNT

In the aforementioned decision, the Venerable Judges of the Southern Administrative Central Court - one of the two intermediate instances of the administrative and fiscal jurisdiction in Portugal - ruled that the mere invocation, by the entity to which access to an administrative document was requested (in this case, a public contract), of a regime of restriction of access to information (foreseen in article 6(6), of LADA - Law of Access to Administrative Documents - Law no. 26/2016, of 22 August), without further explanation on how the disclosure of the required information affects the competitive interest and/or the secrecy about the internal life of the company, does not allow, without further ado, to conclude that the disclosure of such information (relating to the execution of the public contract) may seriously affect the competitive capacity or the competitive interest of the company.

According to article 6(6) of LADA, a third party can only access administrative documents containing commercial, industrial or internal company secrets by written authorisation from the company or by demonstrating to hold a direct, personal, legitimate and constitutionally-protected interest that is sufficiently relevant (within the framework of the principle of proportionality, of the fundamental rights in presence and of the principle of open administration) that justifies such access to information - this constitutes a restriction on the right of free access to administrative documents (which includes the rights of consultation, of reproduction and of information about their existence and content - article 5(1) of the LADA).

The said Court considered that, regarding administrative documents with personal data or secrets about the internal life of companies, the public entity must allow the process to be consulted and make available the requested documents, but must remove the information on reserved matters (excluding/hiding the parts relating to matters covered by secrecy). It was also considered that it is the duty of the requested entity to present, on a case-by-case basis, the justification for the concealment of those specific elements, so that the requesting entity may syndicate this action.

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.

ELECTRONIC NOTIFICATION

Central Economic-Administrative Board, Decision of 20th July 2022, proc. 00/05927/2021/00/00.

The case before the Central Economic-Administrative Board addresses the statute of limitations for the settlement of the Corporate Tax of 2016 and the legality of electronic notifications. The core issue in the case before the Central Economic-Administrative Board focuses on the fact that a paper notification was made to an entity obligated to receive communications exclusively through electronic means.

The case before the Central Economic-Administrative Board focuses on the proper execution of electronic notification in the context of the Corporate Tax settlement for the fiscal year 2016. The claimant entity questioned the legality of the notifications made by the Administration, arguing that these did not comply with the necessary legal requirements and, therefore, there was not a valid notification of the verification procedure that would validly interrupt the statute of limitations for the Administration's right to settle the tax.

Initially, the Board establishes that the inspection actions began on October 30, 2018, through a communication notified via the electronic mailbox associated with the entity's enabled electronic address, complying with the stipulations in articles 14.2 and 41.1 of Law 39/2015 of the Common Administrative Procedure of Public Administrations. This law mandates electronic notifications for certain entities, including the claimant in this case.

The central issue of the dispute is the notification of the rectification agreement of the settlement proposal dated June 10, 2021. This notification was made in paper format by a tax agent, despite the entity being obliged to receive electronic notifications. The entity argued that this paper notification was illegal and that it should have been carried out exclusively in electronic format.

In evaluating this situation, the Board considers Article 3.2 b) of Royal Decree 1363/2010, which allows the Administration to carry out non-electronic notifications for reasons of administrative efficiency, especially in situations where the statute of limitations of the Corporate Tax was about to expire and a period for allegations still had to be granted to the taxpayer. In this case, it was considered that the paper notification of the rectification agreement was legit and effectively interrupted the prescription period, as it was made to ensure the effectiveness of the act to be notified and the knowledge of the act by the interested party.

The Board also considered that there was no formal irregularity in the inspection actions. The appropriate procedure was followed in the signing of the act of disagreement, the mandatory deadlines for submitting allegations were granted, and the regulations were followed in the rectification of the proposal. No violation was identified in terms of defencelessness or irregularity that could affect the validity of the notification of the settlement agreement.

In summary, the Board determined that the paper notification of the rectification agreement, although unusual given the entity's obligation to receive electronic notifications, was a measure justified by the Administration to ensure the effectiveness of the notification in a context where the prescription period was about to expire. This decision underscores the flexibility within certain legal limits for the Administration in choosing the method of notification, prioritizing effectiveness, and compliance with administrative procedures.

Contentious-Administrative Court (single judge) number 3 of Madrid. Case 537/2022, 23rd November, appeal number 451/2021

In this case, a penalty for obstruction by the taxpayer is annulled. The case originated from the fact that the taxpayer had not acted in accordance with what was indicated by the Administration through an electronic notification made available to them without the accompanying notice to the email address.

The issue addressed by the Court involves the review of the legality of electronic notifications made by the Administration in the context of a settlement of the Tax on Constructions, Installations, and Works (ICIO, by its Spanish acronym). The focus of the dispute centres on the imposition of a tax penalty on an entity, under the allegation of serious tax infringement due to resistance, obstruction, excuse, or refusal to comply with the administrative action.

The Court specifically analyses whether the notifications complied with the requirements of Article 43 and Article 41.6 of Law 39/2015 of the Common Administrative Procedure of Public Administrations. According to these provisions, electronic notifications must be made through the electronic headquarters of the Administration and are carried out when their content is accessed. Additionally, it is required that the Administration sends a notice to the electronic de-

vice and/or the email address of the interested party about the availability of the notification.

In this case, the Court observes that while the first notification attempt was correctly carried out both electronically and on paper, with publication in the BOE, the subsequent two electronic requirements did not fulfil the obligation to send a notice to the email of the interested party. This omission created a situation in which the interested party was unaware of when the municipal administration would make the notification of the requirement available in the electronic office.

The Court considered that, although the law and its applicable jurisprudence — which we have highlighted in this section of previous numbers of our magazine — establish that the lack of notice does not prevent the notification from being considered valid, in this specific case the absence of notice created a situation of defencelessness for the taxpayer. This defencelessness was considered serious, particularly due to the high fine imposed because of not attending to the requirements. The Court argues that knowledge of administrative acts is essential to exercise the right of defence and that the lack of compliance with a legal obligation, even if it does not have a direct legal consequence, is relevant in the context of the imposed sanctions.

The Court also highlighted the difference in the notification dynamics between electronic notifications and paper notifications, noting that in electronic notifications the recipient must actively access the electronic headquarters of the issuer to obtain the notification. This difference implies that, in the absence of a notice, the taxpayer may not be aware of the need to access the notification, which hinders their ability to respond appropriately.

In the end, the Court concluded that the lack of notice in electronic notifications could not be considered as an intentional non-compliance with the requirements by the taxpayer. Consequently, the two unattended requirements without sending the notice should not be considered for the grading of the imposition of the sanction. Based on this, the Court partially upholds the administrative appeal filed by the sanctioned entity, annulling the originally-imposed sanction and replacing it with a fine of 300 euros.

Constitutional Court. Case 84/2022, 27th June, appeal number 83/2021.

In the present Judgment, the Constitutional Court declares the citizen's right to effective judicial protection to have been violated due to electronic notifications being sent to an electronic address of which the citizen was unaware, and without proper notification of the availability of these notifications, as it was sent to an incorrect address.

The Constitutional Court's judgment examines an appeal related to the legality of electronic notifications in a sanctioning procedure in the land-transport sector. The appeal challenges several judicial and administrative decisions, including a sanctioning resolution and the rejection of a request for ex officio review, brought by a businessman involved in land-goods transport and his legal successor.

The conflict originates when the appellant submits a declaration in December 2016 to the General Directorate of Transport, complying with the requirement of having an electronic address and signature for communications with clients. However, an error occurred in the transcription of his email address in the register, affecting future electronic notifications.

In January 2018, the land-transport inspection requested documentation from the appellant related to the tachographs of his vehicles. The notices of the availability of the notification in the Enabled Electronic Address for this request were sent to the incorrect email address, resulting in the appellant not receiving the notices and failing to respond, leading to the notification being considered automatically rejected due to the lapse of the ten days established in Law 39/2015.

Subsequently, a sanctioning procedure was initiated against the appellant alleging serious infringements related to the driving and rest times of his vehicle drivers. Again, the notices of availability were sent to the wrong email address, preventing access to the relevant notifications.

In October 2018, a fine of €4,001 for each infringement was imposed, totalling €16,004. The defect in the notice of the availability of the notifications of the administrative acts was repeated, so the taxpayer went on without accessing them.

In May 2019, a demand for payment totalling €18,750.53 was notified to the appellant, corresponding to the imposed fines and corresponding surcharges. The appellant requested a review of null acts under Law 39/2015 in relation to the sanctioning resolution, arguing that he had not received notifications at the email address he had provided, but his request was rejected.

The appellant filed a contentious-administrative appeal, invoking the violation of

his right to effective judicial protection and due process, in accordance with Article 24 of the Spanish Constitution. He argued that the notifications of the sanctioning procedure were not correctly carried out due to the error in the email address and that the administration did not exhaust all means to ensure that he was effectively aware of the notifications.

The Central Contentious-Administrative Court No. 5 issued a rejecting judgment, arguing that the error in the email address was attributable to the appellant and that, as a businessman, he should have been aware of his obligation to interact electronically with the administration. The Supreme Court had previously expressed the same view in similar circumstances, as analysed in previous issues of this publication. In the subsequent appeal, the Judgment of October 2, 2018 (appeal no. 38-2018), of Section Seven of the Contentious-Administrative Chamber of the National High Court, confirmed the Court's Judgment. An appeal for cassation was filed, but it was unadmitted by the order of April 11, 2019, of Section One of the Contentious-Administrative Chamber of the Supreme Court.

In the appeal for protection before the Constitutional Court, the appellant alleges the violation of his right to effective judicial protection and the right to defence, attributing it to both the administration and the judicial body. He maintains that the administration did not exhaust all means to ensure that the notifications reached his knowledge and that the judicial body did not give him the opportunity to contradict the administration's arguments.

The State Attorney, in his allegations, dismisses the violation of the right to defence, noting that the appellant notified an incorrect email address and that such action cannot be considered diligent. He argues that, as a transporter, the appellant was obliged to comply with the requirements demanded by the transport regulations, among them, those stipulated in Articles 43 and 56 of the Law on the Regulation of Land Transport.

The prosecution is interested in the partial estimation of the appeal for protection, declaring that the contested administrative resolutions have violated the appellant's fundamental right to defence inherent to the right to due process under Article 24.2 of the Spanish Constitution, given that the sanctioning resolution was issued without enabling the appellant to have effective knowledge of the electronic communication acts.

In this context, the Constitutional Court determines that the fundamental right to defence and to be informed of the accusation of the appellant, according to Article 24.2 of the Spanish Constitution, has been violated.

The Court bases its decision on the finding that the appellant was not effectively aware of the electronic notifications made at his enabled electronic address, as well as the sanctioning procedure that had been initiated. This lack of knowledge was due to the erroneous transcription of his email address in the register, which led to important notifications not reaching his knowledge. The Court considers that this situation generated a violation of the appellant's right to defence, as he could not adequately exercise his rights in response to the ongoing administrative and judicial actions.

Because of this determination, the Constitutional Court decides:

1) To annul both the administrative and judicial resolutions related to this case, including the sanctioning resolution and the decisions of the Central Contentious-Administrative Court, as well as the order that resolved the nullity incident.
2) To order the retroaction of the actions to the moment prior to the electronic communication of the requirement by the land transport inspection. This measure aims to ensure that electronic communication is carried out in a way that respects the fundamental right of the appellant recognized by the Court.

Constitutional Court, First Chamber, case 147/2022, 29th November, appeal number 3209-2019

In the present Judgment, the Constitutional Court finds that the citizen's right to effective judicial protection have been violated due to electronic notifications being sent to an electronic address of which the citizen was unaware, among other reasons, given that the paper notification indicating the implementation of the electronic notification system was delivered to an unsuitable person.

This judgment before the Constitutional Court concerns the legality of electronic notifications and their impact on the right to effective judicial protection of a company in the context of a provisional VAT settlement. The contentious issue stems from an error in the transcription of the appellant's email address in the register of the State Tax Administration Agency. Despite this error, on this occasion, the Court found no violation of the appellant's right to effective judicial protection.

The regulations under analysis refer to the

requirements for the delivery of notifications to legal entities established in the Regulation governing the provision of postal services, approved by Royal Decree 1829/1999. According to this regulation, the notification to the taxpayer of the electronic platform that will henceforth be used for electronic notifications must be made through a paper notification. These paper notifications, when directed to legal entities, must be transmitted to their representative or an employee of the same, and in this case, the initial notification of inclusion in the enabled electronic address system was received by the daughter of the legal representative of the company, a person with no link to the company.

Afterward, once the electronic notification system was operational, the claimant entity did not access the communications sent by the Tax Agency through its enabled electronic address, and therefore was not aware of the initiation and substantiation of the limited verification procedure nor of the provisional VAT settlement for the fiscal year 2012.

In this context, the Court considers that, although the Tax Agency did not breach the current regulations in the way of carrying out electronic notifications, it also cannot be affirmed that the lack of access to the notifications was due to a lack of diligence by the legal representative of the company. Along these lines, the importance of the documentation whose provision was required through the enabled electronic address is also highlighted, as its lack of provision was determinative in the settlement made.

Thus, the decision of the Constitutional Court is based on the interpretation that, although the company had the obligation to receive communications electronically and the Tax Agency complied with the established electronic notification procedure, the specific circumstances of the case, including the manner in which the initial notification was made and the company's lack of access to subsequent notifications, led to violation of the right of defence that could not be attributed to a lack of diligence by the legal representative of the company.

ELECTRONIC APPLICATIONS

Supreme Court, Third Chamber of Contentious-Administrative Matters, Section 4th, case 224/2022, 22nd February, appeal number 806/2020.

The Supreme Court's judgment focuses on a cassation appeal related to the rectification of errors in applications submitted electronically. Specifically, the judgment establishes doctrine regarding the omission of an electronic signature in these applications and the obligation of the Administration to offer the possibility to rectify such errors, granting a period of ten days for this purpose.

The cassation appeal was filed against the judgment of the High Court of Justice of Andalusia, which dismissed the administrative appeal brought by a claimant regarding her exclusion from a selective process due to the lack of electronic signature in her telemetrically-submitted application. The claimant argued that, despite having completed the form and received a message indicating that her application had been successfully processed, the absence of a final step in the electronic submission process led to her exclusion from the selective process.

The Supreme Court, in analysing the case, referred to the applicable regulations, including Article 68 of Law 39/2015 of the Common Administrative Procedure of Public Administrations, which establishes the duty of the Administration to allow the rectification of defects or the omission of documents in any application submitted by citizens. The Supreme Court's judgment overturns the decision of the High Court of Justice of Andalusia and declares the claimant's right to be given a period by the Administration to rectify the lack of an electronic signature and, once the rectification is made, to be included in the employment pools with the inherent effects thereof.

ELECTRONIC AUCTION SYSTEM

High Court of Justice of Catalonia, Contentious-Administrative Chamber, Section 2nd, Case 149/2022, 21st January, appeal number 404/2019.

The judgment resolves on the nullity of Decree 41/2019 of Catalonia, which regulated the creation and operation of electronic means for the conduct of public electronic auctions by the Catalan Tax Agency, as it falls under state jurisdiction.

The judgment of the High Court of Justice of Catalonia concerns the annulment of Decree 41/2019 of Catalonia, which aimed to create a portal for conducting public electronic auctions for the alienation of seized goods and rights in the executive collection period of public revenues of the Generalitat Administration and Catalan local administration entities.

The challenge to the decree was based, first-

ly, on the violation of the constitutional framework for the distribution of competencies in tax matters. The representation of the General State Administration argued that the conduct of auctions is exclusive and must be carried out through the Auction Portal of the State Agency of the Official State Gazette (BOE).

The contested decree was deemed contrary to the constitutional competencies reserved to the State, particularly those established in Article 149.1 of the Spanish Constitution, which include competencies on regulating the basic conditions that guarantee the equality of all Spaniards, the effectiveness of legal norms, the General Treasury and State Debt, and the foundations of the legal regime of Public Administrations and common administrative procedure.

Furthermore, it was pointed out that Article 100 of the General Collection Regulation (Decree 939/05) was also breached, as it stipulates that the conduct of electronic auctions of seized goods must be carried out exclusively through the Auction Portal of the State Agency of the Official State Gazette, not admitting a similar figure at the autonomous community level.

Thirdly, it was argued that the contested decree violated the Organic Law of Financing of the Autonomous Communities (LOFCA, by its Spanish acronym) and the Law regulating the financing system of the Common Regime Autonomous Communities (Law 22/09), which demand absolute respect for state competencies.

Finally, the legality of the regulation was called into question, indicating that the decree failed to comply with the principles of good regulation established in Law 39/15 of the Common Administrative Procedure of Public Administrations, especially the principles of necessity, effectiveness, proportionality, legal security, and efficiency, by creating an unnecessary duplication of public services and generating higher costs.

The Autonomous Community of Catalonia defended its actions, claiming that it acted within its self-organization competencies recognized by the Statute of Autonomy of Catalonia and its Tax Code, denying the violation of the principles of good regulation.

Faced with the litigation thus presented, the High Court of Justice of Catalonia considered that, although Autonomous Communities have the right to seek financial autonomy, they must comply with the norms that take precedence over others, which are those that make up the block of constitutionality, including the Constitution and the laws that distribute competencies between the State and the Autonomous Communities.

Therefore, it was pointed out that the challenged general provisionviolated the exclusive state competencies in tax matters, especially regarding the "General Treasury," allowing the State to fully regulate its own Treasury and establish common institutions for the different Treasuries.

Given the above, the administrative appeal was fully upheld, declaring the contested Decree null and void for being contrary to the General Tax Law, the General Collection Regulation, and the precepts of the laws distributing competencies.

QUALIFICATION OF PUBLIC EMPLOYEES IN THE FIELD OF ELECTRONIC ADMINISTRATION

High Court of Justice of Galicia, Contentious-Administrative Chamber, Section 1st, Case 816/2022, 2nd November, appeal number 222/202

Need for tasks related to electronic administration to be entrusted to personnel with adequate technological training.

The judgment addresses the nullity of a delegation of functions assigned to a public employee. The conflict originates from an administrative decision by the City Council of Lugo, which assigned an employee, with the status of a permanent labour staff member as a psychologist, tasks related to computer duties in the new municipal transparency portal. The CSIF union, representing the employee, contested this delegation of functions, arguing that the tasks assigned were exclusively for career civil servants.

The Court of First Instance estimated the demand, annulling the administrative resolution, considering that the labour employee could not be legally assigned the entrusted tasks, as they were categorized as bureaucratic functions reserved for public officials.

On appeal, the City Council of Lugo argued that the specific tasks assigned in the contested decree should be in the Service of Attention and Citizen Participation, being part of the duties of the employee's job, and that the employee had already been performing similar services under another designation. However, the High Court of Justice of Galicia dismissed the appeal, confirming the judgment of the first instance.

The Court based its decision on the fact that the functions assigned to the employee could not be performed by labour staff, considering his qualification as a psychologist and the digital competencies and knowledge about electronic

administration required for the assigned tasks. It was noted that these tasks were more suitable for those with qualifications related to computer science and new technologies than for a psychologist.

Furthermore, the Court considered that the regulatory norms did not require that the delegated tasks be performed by civil servants, but that the tasks attributed in the contested resolution could not be performed by labour staff due to their technical and specialized nature.