UNIO - *EU Law Journal*. Vol. 11, No. 1, June 2025, pp. 126-145.
®2025 Centre of Studies in European Union Law
School of Law - University of Minho

Who should be the "controller" of personal data files in the courts? On processing personal data "acting in judicial capacity" and judicial independence. Special reference to the current legislation in Portugal and Spain

Gema Pérez Souto*

ABSTRACT: As it follows from Recital 20 as well as from the delimitation set out in its Article 2 in its material scope of application, the Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR) – is competent to apply to the court's activity and other judicial authorities, stating that "Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities." *The GDPR exempts the processing of personal data* "by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" *[Article 2(2)(d), to which Directive (EU) 2016/680 of 27 April 2016 shall apply]. Recital 80 of the aforementioned Directive states in similar terms to the GDPR that:* "While this Directive applies also to the activities of national courts and other judicial authorities, the competence of the supervisory authorities should not cover the processing of personal data where courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks." *In view of this legal framework, the question of who should hold the status of (data) "controller" in the courts is still not a peaceful question. In this paper we shall develop our argument, pointing out that it should be the judges and courts, who would hold the role of "controller" for the processing of personal data when "acting in judicial capacity" as defined in the recent judgment of the Court of Justice of the European Union (CJEU) of 24 March 2022 in case C-245/20. Finally, we shall make a critical analysis of this question in the current regulation in Portugal and Spain about data protection and the "controller" in the courts ("Responsável pelo Tratamento" in Portuguese; "Responsable del Tratamiento" in Spanish).*

KEYWORDS: Personal data protection in the courts – controller – jurisdictional and non-jurisdictional data files – judicial independence – Portugal and Spain.

* Postdoctoral Researcher - Foundation for Science and Technology (FCT) CEECInd Fellow, DOI 10.54499/CEECINST/00018/2021/CP2806/CT0001, Research Centre for Justice and Governance (JusGov), School of Law of the University of Minho. Academic member - Open Council of Europe Academic Networks (OCEAN).

1. Introduction

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016[1] – General Data Protection Regulation (GDPR) –, applicable as of 25 May 2018, introduced far-reaching data protection reforms, including data protection obligations covering both private entities and public authorities.

According to Article 4 of the GDPR, "*personal data*" means "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*" As it follows from Recital 20 as well as from the delimitation set out in its Article 2 in its material scope of application, the GDPR can apply to the Court's activity and other judicial authorities, stating below that "*Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities.*"

The GDPR exempts[2] the processing of personal data "*by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.*" Article 2(2)(d), to which Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016[3] shall apply, Recital 80 of the aforementioned Directive, states in similar terms to those of the GDPR that: "*While this Directive applies also to the activities of national courts and other judicial authorities, the competence of the supervisory authorities should not cover the processing of personal data where courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks.*"

In the European Union, the right to personal data protection is regulated autonomously in Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) which states that: *"Everyone has the right to the protection of personal data concerning them"* and, consequently, in Article 8 of the Charter of Fundamental Rights of the European Union (CFREU)[4] which states: "*1. Everyone has the right to*

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union (OJEU), 04.05.2016.

[2] The GDPR would apply, however, when the processing of personal data under Directive (EU) 2016/680 is carried out for a purpose other than that for which the processing was initially intended (autonomous processing operation), including, for example, the publication of judgments of the criminal jurisdiction, which would then fall under the competence of the GDPR (and not of Directive 2016/680), See, in this regard, José Luís Lopes da Mota and Gema Pérez Souto, "Publicación *on-line* de las decisiones judiciales en Europa, Derechos Humanos y Protección de Datos a la luz del RGPD: ¿Misión cumplida?", *Revista General de Derecho Europeo (RGDE)* 49 (2019): 16-51.

[3] On the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data and repealing. Council Framework Decision 2008/977/JHA.

[4] "*This Article has been based on Article 286 of the Treaty establishing the European Community and Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31) as well as on Article 8 of the ECHR and on the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has been ratified by all the Member*

the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."

Therefore, this specificity of the right to data protection as a right of an "*autonomous*" nature cannot be understood without the framework in which the foundations of the European Union's model of protection of fundamental rights are laid, such as in its recognition as general principles of the Union[5] and in "*its connection with different sources coming from Europe, such as the Constitutive Treaties themselves, especially the CFREU, national rules (from the Constitutions of the Member States and those corresponding to their common constitutional traditions) and international rules on the protection of human rights, especially the European Convention on Human Rights*."[6] Let us also recall in this respect Article 2 of the Treaty on European Union (TEU) which states that: "*The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail*."

Chronologically preceding all these rules is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), a pioneering international instrument in data protection known as Convention 108+ after the amendments made in 2018[7] and which has as its point of reference the European Convention on Human Rights (ECHR),[8] specifically Article 8 which contains the right to respect for private and family life.[9] And if we talk about the protection of

---

States. Article 286 of the EC Treaty is now replaced by Article 16 of the Treaty on the Functioning of the European Union and Article 39 of the Treaty on European Union. Reference is also made to Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1). The above-mentioned Directive and Regulation contain conditions and limitations for the exercise of the right to the protection of personal data", Praesidium, *Explanations on the Charter of Fundamental Rights* (2007/C 303/02), *Explanation on Article 8,* Official Journal of the European Union (OJEU) 14.12.2007. Let us also recall that with the Treaty of Lisbon, Article 6 of the Treaty on European Union (TEU) would establish that: *"1. The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties (...) The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions..."*

[5] The Treaty on European Union (TEU) states in Article 6(3) that "*Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law.*"

[6] See Alessandra Silveira, "Carta dos Direitos Fundamentais da União Europeia (CDFUE)", in *Enciclopédia da União Europeia*, ed. Ana Paula Brandão, Francisco Pereira Coutinho, Isabel Camisão and Joana Covelo de Abreu (Lisbon: Petrony Editora, 2017): 68. The original citation is in Portuguese.

[7] Through the *Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (adopted at the 128th session of the Committee of Ministers of the Council of Europe in Elsinore, Denmark on 17-18 May 2018).

[8] *European Convention on Human Rights* (ECHR) adopted by the Council of Europe on 4 November 1950.

[9] Article 8 ECHR: *"The right to respect for private and family life. 1. Everyone has the right to respect for his*

fundamental rights in the field of the jurisdictional order, we must also refer to the protection of the rights of the individuals in the field of criminal proceedings which, as Lopes da Mota points out, *"represents a civilisational conquest of the State of Law that temporarily in many ways precedes the specific purpose of the laws of «data protection»."*[10] This guarantee of respect for the private life of the individual currently has a dimension in the normative sphere that exceeds the scope of the right to privacy itself and extends to the realisation of an autonomous right,[11] which is the right to the protection of personal data that also binds all public authorities and, in particular, those who, as is the case of the courts and tribunals, are called upon to protect them.[12]

As a corollary, one should bring to this point Recital 4 of the GDPR which states, in short, that the processing of *personal* data *"should be designed to serve mankind"* and for this reason *"The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."*[13] Article 47 CFREU becomes

private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[10] See José Luís Lopes da Mota, "Cooperação judiciária em matéria penal e protecção de dados pessoais na União Europeia: perspectivas à luz da experiência da Eurojust", in *Estudos em homenagem ao Professor Doutor Jorge de Figueiredo Dias*, ed. Manuel da Costa Andrade and Maria João Antunes (Coimbra: Coimbra Editora, Stvdia Ivridica, 98, vol. I, 2009): 765. The original citation is in Portuguese.

[11] The singularity and autonomy of the right to the protection of personal data, with respect to the right to the privacy of private and family life, as well as its object of protection, has been perfectly defined in the Judgment of the Spanish Constitutional Court (STC 292/2000 of 30 November, Boletín Oficial del Estado, no. 4, 04 January 2001), which continues to be a reference decision. Thus, in legal basis § 6 of the aforementioned judgment, it is stated that: *"The function of the fundamental right to privacy of art. 18.1 CE is to protect against any invasion that may be carried out in that area of personal and family life that the person wishes to exclude from the knowledge of others and from the intrusions of third parties against their will (for all STC 144/1999, 22 July, FJ 8). On the other hand, the fundamental right to data protection seeks to guarantee that person a power of control over his or her personal data, over their use and destination, with the aim of preventing their unlawful trafficking, detrimental to the dignity and rights of the person concerned. Finally, the right to privacy makes it possible to exclude certain data of a person from the knowledge of others, for this reason, as this Court has said (SSTC 134/1999, of 15 July, FJ 5; 144/1999, FJ 8; 98/2000, of 10 April, FJ 5; 115/2000, of 10 May, FJ 4), that is, the power to protect their private life from unwanted publicity. The right to data protection guarantees individuals a power of disposal over such data. This guarantee imposes on the public authorities a prohibition on them becoming sources of that information without due guarantees; and also the duty to prevent the risks that may arise from improper access to or disclosure of that information. But this power of disposal over one's own personal data is worthless if the data subject does not know what data are held by third parties, who holds them, and for what purpose. Hence the uniqueness of the right to data protection, since, on the one hand, its object is broader than that of the right to privacy, since the fundamental right to data protection extends its guarantee not only to privacy in its constitutionally protected dimension under Art. 18.1 EC, but also to what this Court has sometimes defined in broader terms as the sphere of personal assets belonging to the sphere of private life, inextricably linked to respect for personal dignity (STC 170/1987, 30 October, FJ 4), such as the right to honour, expressly mentioned in Art. 18.4 EC, and also, in a very broad expression of Art. 18.4 EC itself, to the full exercise of the rights of the individual. The fundamental right to data protection extends the constitutional guarantee to those data that are relevant to or have an impact on the exercise of any rights of the individual, whether or not they are constitutional rights and whether or not they relate to honour, ideology, personal and family privacy or any other constitutionally protected right."* The original citation is in Spanish.

[12] See Pablo Lucas Murillo de la Cueva, "La protección de datos en la Administración de Justicia", in *Cuadernos de derecho judicial*, no. 9, 2004: 238-239.

[13] Recital (4) of the GDPR continues: *"This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression*

meaningful then by ensuring that everyone whose rights and freedoms guaranteed by the law of the European Union are violated has the right to an effective remedy and to an independent and impartial tribunal previously established by law. We can therefore conclude that the basis of legitimacy of the processing of personal data by the courts finds its original foundation in the rules of the process itself, which are also linked to the protection of human rights as enshrined in the ECHR.

This general legal framework on the subject gives us the basis to develop our arguments on these aspects in this paper. Namely:

(i) The basis of the legitimacy of the processing of personal data by the courts and the modalities of processing in relation to personal data files (jurisdictional and non-jurisdictional Data Files); and

(ii) the figure of the "*controller*" in relation to the activity of the Courts, that is, which persons or bodies are entrusted with the exercise of the usual functions of responsibility linked to the data protection system,[14] focusing in particular on the current regulation of the "*controller*" in the courts, in Spain and Portugal.

We will conclude with some suggestions in relation to questions that still remain open, particularly in Portugal, where the Bill 126/XIII/3rd, which gave rise to Decree 333/XIII – Second Amendment to Law 34/2009, of 14 July,[15] was approved by the *Assembleia da República* on 19 June 2019, but subsequently vetoed on 26 July 2019 by the President of the Republic in the exercise of his right, requesting a new consideration of the Bill. So far, no new proposals to amend Law 34/2009 have been presented, maintaining, as has already been pointed out, an *"undefined definition as to which specific body or bodies within the judicial system exercise the functions that Recital (20) establishes by: «[ensuring] compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations»*."[16]

2. Legal basis for the processing of personal data in the courts

The GDPR already states in Recital 1 the following: "*The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.*"

The investigation activity within the framework of a proceeding and the processing of the personal data[17] of the data subject (the subject facing the proceeding) is in itself an interference[18] in the right to privacy in the first place and, by extension,

---

and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

[14] On data protection regulation in the courts, see Sofia Wengorovius, "Tribunais e Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a proteção de dados (RGPD)", *O Direito*, Ano 155.º, III (2023): 447-481.

[15] The Bill 126/XIII/3rd, approves the legal regime applicable to the processing of data concerning the judicial system that gave rise to Decree 333/XIII – Second Amendment to Law 34/2009, of 14 July –.

[16] Wengorovius, "Tribunais e Regulamento (UE) 2016/679...", 474. The original citation is in Portuguese.

[17] In this regard, see the exhaustive monograph by Juan Alejandro Montoro Sánchez, *Uso y cesión de datos de carácter personal en el proceso penal* (Pamplona: Ed. Thomson Reuters Aranzadi, 2022), which is closely followed.

[18] In this regard, judgments CJEU *Michael Schwarz v. Stadt Bochum*, 17 October 2013, case C-291/12,

in the fundamental right to the protection of personal data guaranteed by Article 8 of the CFREU, so we are faced with the possible communication or transfer of data[19] that finds the judicial body as the recipient of the personal data and which, precisely due to this interference, has come to require the establishment of specific protection mechanisms.[20]

Before it became imperative to include this "*new*" right, which meant the protection of personal data in criminal proceedings, linked to the use of computer equipment and new technologies, in order to establish specific rules aimed at protecting the rights of the individual in the face of the increasingly intensive and extensive processing of personal data,[21] there existed the rules of criminal procedure relating to privacy which, although they do not constitute in themselves, as we have already pointed out, rules of data protection *"have a similar purpose and are based on identical principles, such as those of legality, necessity, adequacy and proportionality derived from the Convention on Human Rights*."[22]

This inseparable binomial of data protection and its imperative insertion in the process has a direct impact on the rules of the process and its organisation, on the purposes of the processing and on the limitation of data according to the different

ECLI:EU:C:2013:670 and *Digital Rights Ireland Ltd v. Minister for Communications and others*, 8 April 2015, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, which agree that these access and communication operations constitute an interference with the fundamental right to the protection of personal data protected by Article 8 of the Charter of Fundamental Rights of the European Union, because they constitute processing of personal data. The CJEU (Grand Chamber) expressed the same view in its Opinion 1/15 of 26 July 2017, (EU-Canada PNR Agreement) at paragraphs 124 and 126, where it stated that "(...) *the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental right enshrined in Article 7 of the Charter, whatever the subsequent use of the information communicated. The same can be said of the storage of personal data and access to such data with a view to their use by public authorities",* cited in Juan Alejandro Montoro Sánchez, "La aportación de datos de carácter personal de terceros al proceso penal" in *Revista Derecho y Proceso*, no. 1 (June 2022): 34. The original citation is in Spanish.

[19] On this issue, see Carlos Trujillo Cabrera, "Las bases de legitimación del tratamiento de datos personales. En especial, el consentimiento", in *Protección de datos, responsabilidad activa y técnicas de garantía*, ed. Juan Pablo Murga Fernández, María de los Ángeles Fernández Scagliusi, Manuel Espejo Lerdo de Tejada (Madrid: Editorial Reus, 2019).

[20] Lopes da Mota, "Cooperação judiciária em matéria penal...", 764.

[21] Consider, for example, the latest developments in the digitisation of justice, which will lead to a massive increase in the processing of personal data. Without wishing to be exhaustive, the e-Codex on the cross-border exchange of data (Regulation 2022/850); e-evidence or electronic evidence (Regulation 2023/1543 and Directive 2023/1544) and, in short, the digitisation of judicial cooperation (Directive 2023/2843 and Regulation 2023/2844). Well before these regulations, Declaration 21 annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 on the protection of personal data in the field of judicial cooperation in criminal matters and police cooperation already recognised *"that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields*." On Digital Justice, see the essential book by Antoine Garapon and Jean Lassègue, *Justice Digitale. Révolution graphique et rupture anthropologique* [Paris: Presses Universitaires de France/Humensis (puf), 2018]. Another question, which is not the subject of study in this paper, but which is already being raised, is the relation of privacy and data protection in the use of artificial intelligence (AI). In this regard, and on the need and explanation of why it will be necessary to apply "containment" in artificial intelligence, see the revealing book by Mustafa Suleyman, current CEO of Microsoft AI and former vice-president of product management and AI policy at Google, *A próxima Vaga. Inteligência artificial, poder e o grande desafio do século XXI* (Lisbon: Clube do Autor, 2023).

[22] Lopes da Mota, "Cooperação judiciária em matéria penal...", 764. The original citation is in Portuguese.

phases of the procedure, being necessary to combine also the secrecy of justice and the publicity of the procedure with the right to privacy, with the principle of judicial transparency and the "*need to know*" principle[23] arising also other no less essential questions such as the publication of judicial decisions and, consequently, the pseudonymisation of personal data.[24]

We can therefore conclude, as a first conclusion, that the legitimacy of data processing by the courts finds its primary basis in the rules of the process itself, which are also linked to the protection of human rights as set out in the ECHR, as we have already pointed out in the introduction to this paper.

Secondly, in order to develop our line of argument in relation to the legal basis for the processing of jurisdictional data by courts, let us look at what happens with the Directive 2016/680/EU for the criminal courts. Actually, it would be necessary to resort to the general scope of Article 4(1)(a) of Directive 2016/680/EU, consistent with the element of the "*lawfulness*" of the processing as a backbone element, and which must be verified, in any case, as a guarantee of respect for the right of the data subject, establishing that "*1. Member States shall provide for personal data to be: (a) processed lawfully and fairly.*" Thus, the general principle established in the aforementioned Directive is specified in its Article 8(1): regarding the lawfulness of processing: "*1. Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.*"[25]

Continuing with our line of argument, it is necessary to articulate the above to establish the argument's basis by referring to Article 8(2) of the Directive, which establishes that the processing of data must be expressly provided for in the legal system of the Member States by means of a reservation of law, "*shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.*"

In short, processing is lawful only in so far as it is provided for by law and in so far as it is necessary for the stated purposes and is carried out by a competent authority in the exercise of its functions[26] and which acquires significance, according to the EU legal framework preceding this point, by the mandatory obligation to frame this interference as a measure restricting fundamental rights in the principle of proportionality.

Consistently, and to complete this reference, we should turn to Recital 35 of Directive 2016/680/EU which states that: *"In order to be lawful, the processing of personal data under this Directive should be necessary for the performance of a task carried out in the public interest by a competent authority based on Union or Member State law for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Those activities should cover the protection of vital interests of the data subject. The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them*

[23] José Luís Lopes da Mota, Presentation at the *Conference on Digitisation of Justice in the European Union: Current State and Future Challenges*, Escola de Direito da Universidade do Minho, Braga, 11 October 2024.

[24] See footnote 2 of this paper.

[25] See also Articles 9 and 1.

[26] Joaquín Delgado Martín, "La protección de datos personales en el proceso penal: Directiva 2016/680", *Revista de jurisprudencia*, no. 2 (2019): 6. The original citation is in Spanish.

to require or order natural persons to comply with requests made." For Delgado Martín,[27] the principle of the lawfulness of data processing in the criminal jurisdiction is determined exclusively by the concurrence of three elements: *"the contribution to one of the purposes of the Directive, the nature of the controller and the legal authorisation to carry out processing operations. Or, in other words, the processing is lawful as long as it is provided for by law, is limited to one of the purposes referred to in the scope of application of the Directive and is carried out by some of the subjects contemplated as controllers, the competent authorities*."[28]

Therefore, the last step of this legal basis for data processing by all jurisdictional orders, whether or not they are criminal courts, is due to the exclusive attribution to judges and magistrates of the exercise of jurisdictional power to judge and enforce what has been judged, which is identified with a public power of the State that emanates from popular sovereignty and whose exercise has been entrusted to the members of the Judiciary by virtue of the Constitution.[29] As Montero Aroca points out, "*The jurisdictional role consists of protecting the legitimate rights and interests of individuals through the application of the law*" and is definitively linked to the impartiality of the courts[30] that the exercise of their jurisdictional authority. This

---

[27] *Ibidem.*

[28] In the same vein Recital 11 of the Directive , which requires that *"In order to be lawful, the processing of personal data under this Directive must be necessary for the performance of a task carried out in the public interest by a competent authority under Union or Member State law for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the protection and prevention of threats to public security"* and Recital 35 of the Directive in relation to the provision of data by data subjects in the framework of the process, "*The exercise of the functions of prevention, investigation, detection or prosecution of criminal offences which the law institutionally confers on the competent authorities enables them to require or order natural persons to comply with requests addressed to them. (...) When the person concerned is required to comply with a legal obligation, he has no real freedom of choice, so that his response cannot be regarded as constituting a free expression of his will."*

[29] Article 117(1) and 3 of the current Spanish Constitution establishes that: *"1. Justice emanates from the people and is administered in the name of the King by Judges and Magistrates who are members of the judicial power, independent, irremovable, responsible and subject only to the rule of law: (...) 3. The exercise of jurisdictional authority in all types of proceedings, judging and enforcing what is judged, corresponds exclusively to the Courts and Tribunals determined by the laws according to the rules of competence and procedure established therein."* Article 202(1) and 2 of the Constitution of the Portuguese Republic states the following: *"1. The courts are the organs of sovereignty with competence to administer justice on behalf of the people. 2. In the administration of justice, the courts are responsible for ensuring the defence of the legally protected rights and interests of citizens, repressing the violation of democratic legality and settling conflicts of public and private interests."* The original Articles are in Spanish and in Portuguese respectively.

[30] Regarding the impartiality of judges and courts: *"The impartiality of the judge, in order to be able to fulfil his intrinsic function, is complete with respect to the parties (unlike the public prosecutor's office). Finally, the judge must, as defined by Italian doctrine and the Italian Constitution, be vested with the quality of terzietà. That is to say, the judge is a third party (terzo), separate and "alien" to the proceedings and also reinforced in his impartiality. Article 111 of the Italian constitution states that "all court trials are conducted with adversary proceedings and the parties are entitled to equal conditions before an impartial judge in third party position (giudice terzo e imparziale). As the Italian doctrine rightly recalls, both terms must be combined to reinforce the idea of the judge's absolute detachment from litigation, from whatever angle one looks at it, so that the trial is only truly fair when the judge is third and impartial, because terzietà and impartiality are the cornerstones for an effective exercise of jurisdiction, to the point that if one of the two requirements is missing, it could almost be said that we are in the presence of a mock trial".* See Gemma Pérez Souto, «The independent and impartial judge as the sole issuing "judicial authority" of the European arrest warrant versus the public prosecutor›s office – a divergent analysis vis-à-vis the case law of the Court of Justice of the European Union (CJEU)», *JusGov* Research Paper no. 2022-16 (December 21, 2022), 8, available at SSRN: https://ssrn.com/abstract=4332740.

impartiality supposes, in short, as Montero Aroca goes on to say, "*the absence of any design or intention on the part of the judge to place his jurisdictional role at the service of the particular interest of one of the parties*."[31]

Finally, if we refer to the particularity of the processing of personal data in criminal proceedings, it is also justified, in a democratic state governed by the rule of law, on the basis of Article 6 of the CFREU[32] which enshrines the right to liberty and security (corresponding to the same rights enshrined in Article 5 of the ECHR).[33] Therefore, the *ius puniendi*[34] of the State, which is the *last ratio* in the exercise of a general public function, thus contributes to the maintenance of public peace and security (public aims) with others of an individual nature (such as reintegration), and must always be oriented towards the fundamental rights and dignity[35] of the person, which *"is not only a fundamental right in itself, but constitutes the very basis of fundamental rights (...) and forms part of the rights enshrined in the present Charter (CFREU). It may not therefore be infringed, even in the case of a limitation of a right*."[36]

3. The "controller" of personal data files in the courts. Processing personal data "acting in judicial capacity" and judicial independence

Having previously analysed the basis for the legitimisation of data processing by the courts, the next point to be addressed will therefore be the figure of the "*controller*", *i.e.* which persons (or which bodies) will be entrusted with the exercise of the usual functions of responsibility for processing linked to the data protection

---

[31] Juan Montero Aroca, "Derecho a la imparcialidad judicial – Comentario al artículo II-07 del Tratado por el que se establece una Constitución para Europa y al artículo 6.1 del Convenio Europeo de Derechos Humanos", *Revista Europea de Derechos Fundamentales*, 7 (2006): 69. The original citation is in Spanish.

[32] As Lopes da Mota points out, it should be recalled that: *"Convention 108 of the Council of Europe allows for derogations from the principles laid down in Articles 5, 6 and 8 «except such as is in accordance with the law and is necessary in a democratic society (a) in the interests of national security, public safety or the economic well-being of the country or for the prevention of disorder or crime; (b) or for the protection of the rights and freedoms of others» [(article 9 (2)]*." Lopes da Mota, "Cooperação judiciária em matéria penal...", 771. The original citation is in Portuguese.

[33] Article 5(1) ECHR: *"Article 5 - Right to liberty and security 1. Everyone has the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law (...)*."

[34] Montoro points out that: "*Gimeno Sendra, citing Fenech, Viada and Montero, conceives of criminal proceedings as the instrument that the Jurisdiction has for the exclusive application of the ius puniendi of the State. On the other hand, it is clear from the case law of the CJEU that the fight against international terrorism for the maintenance of international peace and security is an objective of general interest of the Union, in this sense, the judgments in Kadi and Al Barakaat International Foundation v. Council and Commission, C-402/05 P and C-415/05 P, paragraph 363, and Al-Aqsa v. Council, C-539/10 P and C-550/10 P, paragraph 130. As well as the fight against serious crime to guarantee public safety and freedom guaranteed in art. 6 of the CFREU, in this sense, the Tsakouridis judgment, C-145/09, paragraphs 46 and 47 (...)*." Montoro continues quoting Gimeno Sendra, when he states that *"the function of criminal proceedings cannot be identified exclusively with the application of ius puniendi, and this, for the simple reason that it is also intended to declare the right to liberty of the innocent citizen*." See Montoro Sánchez in *Uso y cesión de datos de carácter personal en el proceso penal...*, footnotes 780 and 781. The original citation is in Spanish.

[35] In judgment CJEU *Kingdom of the Netherlands v. European Parliament and Council of the European Union*, 9 October 2001, case C-377/98, ECLI:EU:C:2001:523, it is confirmed that the fundamental right to human dignity is part of the law of the Union.

[36] Praesidium, *Explanations on the Charter of Fundamental Rights*, (2007/C 303/02), *Explanation on Article 1.*

system in the sphere of the Administration of Justice, specifically in the courts. To do so, it will be necessary to turn first to the definition of the "*controller*", to conclude later with those who hold this competence in the courts, choosing for this purpose as a reference, who holds such a competence in Portugal and in Spain, according to the legislation of these respective countries, and in which we shall analyse our position in this respect.

According to Article 4(7) GDPR, *"controller*" is defined as "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*." To uphold the rights and freedoms of natural persons with regard to the processing of personal data, as set out in Recital (78) of the GDPR, appropriate technical and organisational measures are required to be taken in order to ensure compliance with the requirements of the Regulation, by adopting internal measures that comply with "*the principles of data protection by design"* and "*by default*." These include the earliest possible pseudonymisation of personal data and transparency in the functions and in the data processing itself *"allowing data subjects to monitor data processing and the controller to create and enhance security features*."

Furthermore, Article 5(2) of the GDPR explicitly states that *"controllers shall be responsible for ensuring compliance with paragraph 1*." This refers directly to the fundamental principles relating to data quality, *inter alia*, the principle laid down in Article 5(1)(a) that *"personal data are processed fairly and lawfully"*, which in practice means that all provisions laying down conditions for lawful processing point directly to the controller, even if this is not always clearly formulated. The controller therefore is responsible for compliance with Article 5(1) GDPR (Principles relating to the processing of personal data) and must be *"able to demonstrate this"* (*"accountability"*).[37] It is, in short, *the raison d'être* of the controller to ensure that the controller's own responsibility for data processing is clearly defined and can be effectively enforced.[38]

On the other hand, it will then be necessary to refer to the principles of Article 5 of the GDPR in relation to Articles 6 and 9, which operate in practice as the *"Constitution of the GDPR"*[39] (having its origin in Article 5 of Convention 108 and Article 6 of Directive 95/46/EC) and are as follows: the principle of lawfulness, i.e. provided by law (data must be processed *"lawfully, fairly and in a transparent manner"*) articulated as a fundamental axis in relation to the guarantee of the respect of the data subject's right,[40] *"collected for specified, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes"*; principle of data minimisation (adequate, relevant and limited) and accuracy (accurate and, where necessary, kept

[37] In this sense, Sofía Wengorovius points out that: "*In accordance with the principle of accountability, the data controller is responsible for compliance with the legal principles set out in Article 5.1 of the GDPR and must be able to verify this (cf. Articles 5.2, 24 and 25*). *To this end, it must implement the appropriate technical and organisational measures to ensure and be able to prove that the processing is carried out in accordance with the Regulation."* See Wengorovius, "Tribunais e Regulamento (UE) 2016/679", 457. The original citation is in Portuguese.

[38] See also Article 24 GDPR.

[39] Alexandre Sousa Pinheiro and Carlos Jorge Gonçalves, "Comentário ao artigo 5 RGPD (Princípios relativos ao tratamento de dados pessoais)", in *Comentário ao Regulamento Geral de Proteção de Dados*, ed. Alexandre Sousa Pinheiro (Coimbra: Almedina, 2018): 205.

[40] Lopes da Mota, Presentation at the *Conference on the Digitisation of Justice...*

up to date); limitation of data retention for the time necessary for the use of the purposes for which they were collected and without prejudice to pseudonymisation and finally the principle of integrity and confidentiality (security, protection against unauthorised or unlawful data processing, against loss, destruction or damage and, ultimately, with the necessary recourse to appropriate technical and organisational measures).

If we talk about Directive 2016/680/EU in the criminal field, we must remember that the principle of fairness also entails the prohibition of automated decision-making[41] in the sense of Article 11(1) *"based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her."* Article 11 adds *"unless authorised by Union or Member State law to which the controller is subject and which provides for appropriate measures to safeguard for the rights and freedoms of the data subject*." It concludes by confirming the essential role of the controller in upholding the fundamental rights of data subjects, stating that data subjects have "*at least the right to obtain human intervention on the part of the controller."*

As a consequence of the above principles, the rights of the data subject, which are contained in Chapter III of the GDPR (and Chapter VIII of the GDPR in relation to possible remedies such as claims or legal action), are inevitably linked to the right to obtain human intervention,[42] the right of the controller to access,

[41] In the same vein, Lopes da Mota, Presentation at the *Conference on Digitalisation of Justice...*

[42] In the GDPR, the data subject's right of access includes that the data subject "*has the right of access to his or her personal data and to the following information*": "(...) *Article 15(h): the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*." The aforementioned Article 15(1)(h) of the Regulation in relation to Article 22 of the Regulation presents certain difficulties of interpretation in real cases and has required recent jurisprudential interpretation in which the defence of the fundamental rights of the data subject has prevailed, concluding in the protection of these rights contained in the articles of the CFREU. In this regard, and on the concept and characteristics of "*automated decision-making*", see judgment CJEU *SCHUFA Holding and others (Scoring)*, 7 December 2023, case C-634/21, ECLI:EU:C:2023:957. On the other hand, it is also worth noting that in relation to the figure of the controller, that Advocate General Pikamäe in his Opinion issued in this judgment considered that "*real objective of Article 15(1)(h) of the GDPR is to ensure that data subjects obtain information in an intelligible and accessible form in accordance with their needs*" (paragraph 57), relating this in the light of Article 12(1) of the GDPR which states that "*the controller shall take appropriate measures to provide the data subject with any information [...] in a concise, transparent, intelligible and easily accessible form, in clear and plain language*." In a similar vein to that referred to above on automated decisions, Advocate General De La Tour has recently expressed himself in his opinion delivered on 12 September 2024 in case C-203/22, in respect of which, at the time of writing, the CJEU had not yet delivered its judgment, and the Advocate General states: *"In the cases referred to in Article 22(2)(a) and (c) of the Regulation, the controller shall at least take measures in relation to the data subject's right to obtain human intervention, to express his point of view and to contest the decision. In the context of the present case, the national court emphasises the link between the right of access provided for in Article 15(1)(h) of the Regulation and those rights of the data subject to express his point of view and to challenge the automated decision."* (paragraph 49). According to *the Court, the enhanced requirements laid down by the GDPR as to the lawfulness of automated decision-making and the additional information obligations of the controller and the related additional rights of access of the data subject are explained by the purpose pursued by Article 22 of that regulation consisting of protecting individuals against the particular risks to their rights and freedoms represented by the automated processing of personal data, including profiling."* (paragraph 50). See Bart Custers and Anne-Sophie Heijne, "The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice", *Computer Law & Security Review*, volume 46 (September 2022): 105727, https://doi.org/10.1016/j.clsr.2022.105727; Tiago Sérgio Cabral, "AI and the right to explanation: three legal bases under the GDPR", in *Data Protection and Privacy*, volume 13, *Data Protection and Artificial Intelligence* (London: Bloomsbury Publishing, 2022); and Andrew D. Selbst and

rectification and erasure; of restriction of processing (purpose of the data and, as mentioned above, data minimisation); the right to exercise the rights and verification by the supervisory authority in case of refusal) and the right to data security and to information about a possible breach of data security (with the consequent obligation to implement technical and organisational measures or chronological records).

As can be seen, the "*controller*" is considered to be at the core of the provisions on prior notification and controls. Montoro adds that *"the right-duty of information is recognised, being an element that contributes to the fullness of control over the personal data itself"*, adding that it is not surprising that the controller is in principle liable for the damage resulting from unlawful processing (Article 23)."[43]

The rights of data subjects may be limited under certain circumstances, as set out in Article 23 GDPR, as we have seen, but always in accordance with the principle of proportionality and respect for fundamental rights: "*1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: (...)*" and the Article lists[44] a series of situations[45] among which it is worth highlighting: *"(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (...) (f) the protection of judicial independence and judicial proceedings*."

3.1. The processing of data for «jurisdictional purposes and for "non-jurisdictional purposes". The view of the CJEU on the definition of "acting in judicial capacity" in case C-245/20 of 24 March 2022 and the protection of judicial independence

Having seen the functions and characteristics of the (data) controller in general, the question that arises at this point more specifically is what types of data are processed and who holds the status of "*controller*" when it comes to courts.

Firstly, before determining who is/should be the "*controller*" when it comes to courts, it will be necessary to determine the processing modalities in relation to the aforementioned processing operations carried out by the courts. Article 55(3) GDPR, when talking about the supervisory authorities, states that *"they shall not be competent to supervise processing operations of courts acting in their judicial capacity.*" In other words, from the definition provided in the aforementioned Article, it can be deduced that there are personal data processing operations within the courts that are carried out in the exercise of their judicial function and others that are not carried out in the

Julia Powles, "Meaningful information and the right to explanation", *International Data Privacy Law*, vol. 7, no. 4 (2018): 233-242, https://doi.org/10.1093/idpl/ipx022.

[43] See Montoro Sánchez in *Uso y cesión de datos de carácter personal en el proceso penal...*, see footnotes 796-797. The original citation is in Spanish.

[44] Article 23(e) extends a possible limitation, provided that such limitation *"respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society*", to *"other important objectives of general public interest of the Union or of a Member State (...).*" See, on this question, judgment CJEU *Peter Nowak v. Data Protection Commissioner*, 20 December 2017, case C-434/16, ECLI:EU:C:2017:994.

[45] On the limitations contained in Article 23 GDPR, see European Data Protection Board, *Guidelines 10/2020 on restrictions under Article 23 GDPR*, version 2.1 updated 13 October 2021.

exercise of their judicial function, which we call data for *"jurisdictional and non-jurisdictional purposes"* which arise as a result of the normal course of the procedure.

This means, therefore, that it is not possible to conceive, as we have already mentioned, the development of a judicial procedure without the generation of different data processing activities from the parties and from the various subjects that intervene from different aspects in the process in the development of its processing. As Montoro points out, in relation to criminal proceedings: "*every process begins with the collection of the data incorporated in the initiating act and attached documents; it continues with their orderly registration in the electronic judicial file and even in the physical file printed on paper; continuing with the communication of the file to the other parties in order to carry out the appropriate mandatory transfers; furthermore, given the increase in cross-border litigation or criminality and the establishment of conventions and rules that facilitate judicial cooperation for the exchange of information, the operations of cession, exchange and transfer of data are usual*."[46]

The distinction of data processing operations within the courts[47] for "*jurisdictional*" and "*non-jurisdictional*" purposes has been in need of interpretation[48] and, consequently, a definition linking the "*jurisdictional*" purpose of data processing with the exercise of judicial independence by the courts.

Finally, the judgment of the CJEU of 24 March 2022 in case C-245/20[49] clarified this matter by stating in its legal grounds § 32 and § 33 that: "*As the Advocate General observed in points 80 and 81 of his Opinion, it is apparent from the very wording of recital 20 of Regulation 2016/679, and in particular from the use of the expression 'including', that the scope of the objective pursued by Article 55(3) of that regulation, consisting in safeguarding the independence of the judiciary in the performance of its judicial tasks.* Which implies, as a general rule, "*that judicial functions are exercised wholly autonomously, without the courts being subject to any hierarchical constraint or subordinate relationship and without taking orders or instructions from any source whatsoever, thus being protected from any external intervention or pressure liable to jeopardise the independent judgment of their members and to influence their decisions. Observance of the guarantees of independence and impartiality necessary under EU law requires rules in order to dispel any reasonable doubt in the minds of individuals as to the imperviousness of the body in question to external factors and its neutrality with respect to the interests concerned*."

The definition of data processing for jurisdictional purposes is defined by the CJEU in the sense that, by default, it should be understood in a *"broad"* manner, reaffirming the exclusion of the competence of the supervisory authority, on the understanding that, otherwise, it would imply an interference with judicial independence. Thus: "*(...) the reference in Article 55(3) of Regulation 2016/679 to processing*

[46] See Montoro Sánchez in *Uso y cesión de datos de carácter personal en el proceso penal...*, 730. The original citation is in Spanish.

[47] On the protection of personal data as a fundamental right in the courts, see Artemi Rallo Lombarte, "La garantía del derecho constitucional a la protección de datos personales en los órganos judiciales", *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, no. 5 (2009): 97-116.

[48] According to Wengorovius *"These (...) specificities in the application of the GDPR to the activity of the courts lead to many practical difficulties, as we have tried to enumerate and develop, questions that are difficult to answer and feasible, which even leads to the question of -what was the spirit of the EU legislator in providing for this applicability."* See Wengorovius, "Tribunais e Regulamento (UE) 2016/679...", 481. The original citation is in Portuguese.

[49] Judgment CJEU *X and Z v. Autoriteit Persoonsgegevens*, 24 March 2022, case C-245/20, ECLI:EU:C:2022:216.

operations carried out by courts 'acting in their judicial capacity' must be understood, in the context of that regulation, as not being limited to the processing of personal data carried out by courts in specific cases, but as referring, more broadly, to all processing operations carried out by courts in the course of their judicial activity, such that those processing operations whose supervision by the supervisory authority would be likely, whether directly or indirectly, to have an influence on the independence of their members or to weigh on their decisions are excluded from that authority's competence."[50]

Therefore, it is concluded that the processing of data for "*jurisdictional purposes*"[51] (or *"acting in judicial capacity"*) encompasses all processing of personal data that takes place as a consequence of the exercise of jurisdictional powers by judicial bodies. In other words, a jurisdictional purpose is attributed to any processing of data that takes place in the course of judicial proceedings, regardless of the jurisdictional order in which it is carried out.

On the contrary, any processing of personal data carried out within the scope of the courts whose purpose is not inextricably linked to the processing of a specific judicial procedure according to the procedural rules, would, in contrast, have the characteristic of *"non-jurisdictional"* (in short, it would be that processing of data in which the jurisdictional power is not exercised, although the person carrying out the processing is a judge or court). In this sense, a *"non-jurisdictional"* data processing would be carried out on those acts of an administrative nature necessary for the management or governance within the courts or tribunals. Among them, mention may be made of "*cases relating to the employment relations of judges, magistrates, legal officers of the Administration of Justice and the staff assigned to the judicial office or to other procedures provided for in the legislation, such as complaints, inspection of courts, reports, disciplinary proceedings, governmental agreements, etc.*"[52]

4. The "controller" of personal data files in the courts in Portugal and in Spain: a critical view

Having clarified this distinction, it is now necessary to determine to whom the role of data controller corresponds in the courts, who would be the "*controller*" of jurisdictional and non-jurisdictional files and, specifically, to establish the current state of play in Spain and Portugal, as these are the countries chosen for analysis.

Beginning with Spain and following Montoro, he gives an exhaustive account[53] of the different legal frameworks that have successively dealt with the regulations on

[50] §34 *Ibidem.*

[51] In the Spanish legal system, as Montoro indicates, this distinction had already been foreseen and thus: "*Article 236 ter of the Organic Law of the Judiciary (LOPJ) in the wording given by Organic Law 13/2015, introduced for the first time in a regulation with legal rank a logical classification of the different types of processing of personal data that may be undertaken within the Administration of Justice, an aspect with special significance, since the classification in which a certain processing may be placed, will correspond to the application of a certain legal regime. This precept specified, given that currently, after the reform brought about by Organic Law 7/2021, this distinction is included in Article 236 bis of the same legal body, that the courts may process personal data for two types of purposes: jurisdictional and non-jurisdictional"*, See Montoro Sánchez, *Uso y cesión de datos de carácter personal en el proceso penal...*, 787.

[52] *Ibidem*, 789.

[53] See in particular, Chapter III (Régimen Jurídico del Derecho a la Protección de Datos en la Administración de Justicia) - VII (Atribución de los cargos de responsabilidad en la Administración de Justicia) - 1. (Responsabilidad de los ficheros jurisdiccionales), Montoro, *Uso y cesión de datos de carácter personal en el proceso penal...*

data protection in the sphere of the Administration of Justice and which, certainly at various times, have not contributed much to clarifying who holds the position of data controller in the courts, and in some cases the successive modifications of the Articles of the Spanish Organic Law of the Judiciary (LOPJ)[54] to adapt them to national legislation or as a consequence of the transposition of European Directives or the application of the GDPR have contributed to the confusion.

After several amendments, the situation seemed to be resolved with the amendment of the LOPJ by Organic Law 7/2015[55] with a regulation with the status of law, defining the assignment of the functions of "*controllers*" in the Administration of Justice [in Article 236(6) LOPJ], which is now repealed. As Montoro states, under the wording of this Article, *"the rules for determining the functions of responsibility for both judicial and non-jurisdictional files held in the Administration of Justice were laid down in a differentiated manner (...) Thus, for judicial files, the body or judicial office before which the procedure in which the data subject's data are processed was officially placed at the head, as data controller."*[56]

However, Article 236(6) LOPJ would later be repealed by Spanish Organic Law 7/2021[57] and now, after the amending, it is necessary to turn to Article 236(2) of the LOPJ which establishes the following: "*1. The processing of personal data may be carried out for jurisdictional or non-jurisdictional purposes. The processing of data included in the processes whose purpose is the exercise of jurisdictional activity shall be for jurisdictional purposes. 2. The processing of personal data in the administration of justice shall be carried out by the competent body and, within it, by the body with the competence attributed to it by whoever has the competence according to the regulations in force*." As can be seen in number 2 of this Article, the expression "*by whoever has the competence according to the regulations in force*", which is open-ended, does not contribute to clarifying the issue. This has led to a wide-ranging discussion in the doctrine[58] with contradictory positions, which have not led to a unanimous solution in practice either.

However, we agree with Montoro that the responsibility for processing is held by each of the Courts and Tribunals with regard to data for "jurisdictional purposes", and we consider it more appropriate, according to the role it plays, that it should be the Justice Administration Lawyer – formerly known as the Judicial Secretary (natural person) – who assumes the function of *"controller"* in relation to data for *"non-jurisdictional"* purposes, since the role of controller would generally be attributed to the Judicial Office of which it forms part. Montoro points out in support of his thesis with regard to the processing of data for "*jurisdictional*" purposes by each of the courts and tribunals, that *"basically because we are in a situation in which the legislator made use of the power provided for in EU data protection legislation that allowed the latter to directly designate the data Controller."*[59]

---

[54] Henceforth, in the interest of clarity and understanding, translations into English of Spanish and Portuguese laws, and other relevant official documents, were done by the author.

[55] Spain, Organic Law 7/2015, of 21 July, which amends Organic Law 6/1985, of 1 July, on the Judiciary (BOE, no. 174, of 22 July 2015).

[56] See Montoro, *Uso y cesión de datos de carácter personal en el proceso penal...*, 819.

[57] Spain, Organic Law 7/2021, of 26 May, on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal sanctions (BOE, no. 126 of 27/05/2021).

[58] On the different doctrinal positions and their arguments on this question, See Montoro, *Uso y cesión de datos de carácter personal en el proceso penal...*, 836.

[59] *Ibidem*, 831.

In short, processing is lawful only in so far as it is provided for by law and in so far as it is necessary for the purposes stated and is carried out by a competent authority in the exercise of its functions, and which acquires significance, according to the EU legal framework, by the mandatory obligation to frame this interference as a measure restricting fundamental rights in the principle of proportionality, among others, as stated in the CFREU, and for this reason, only judges and courts with the quality of an independent and impartial authority can be attributed this function. It should be remembered that, for the purposes of the data subject who hold the personal data, the designation of judges or the courts as the data controller makes it possible to identify unequivocally before whom they can exercise their respective rights in accordance with the competences of the data controller established in the legislation in force.

Montoro also distinguishes, in an aspect that seems to us to be clarifying, that is, the ownership of the data controller with respect to the *"formal"* dimension of the data controller (Judicial Office or Courts) as opposed to the *"material"* dimension, which means that in practice neither the Judge or Magistrate nor the Justice Administration Lawyer has effective decision-making capacity in terms of the purposes and means of processing, since in Spain, the majority of the Autonomous Communities that have assumed the transfer of management in the field of justice provide the judicial bodies with means and personnel. For its part, as the author recalls, "*the Ministry of Justice, in addition to providing such means to the territories that have not made use of the subrogation clause, specifically provides the Lexnet tool, which has become the main system for communications between the judicial bodies and the different professionals of the Administration of Justice*." Consequently, this *"material"* dimension, in the expression used by Montoro, would assign both the Autonomous Communities and the Ministry of Justice in this case, the quality of "*processor*"[60] [according to the definition contained in Article 3(9) GDPR].

In Portugal, the current situation regarding the status of data controller in the Courts is as follows:[61]

The Bill 126/XIII/3rd, which approves the legal regime applicable to the processing of data concerning the judicial system that gave rise to Decree 333/XIII – Second Amendment to Law 34/2009, of 14 July –, would be approved by the *Assembleia da República* on 19 June 2019,[62] but subsequently vetoed on 26 July 2019 by the President of the Portuguese Republic in the exercise of his right, requesting a new consideration of the Bill. The right of veto exercised by the President of the Portuguese Republic, was based primarily on the report issued by the *Conselho Superior da Magistratura* (CSM), alerting on various questions, which in their opinion, meant that there was a lack of conformity of the referred Bill with the GDPR. We draw attention to the fact that so far, no new Bills to amend Law 34/2009 have been submitted.

It is not the purpose of this paper to go into the full extent of the aforementioned report of the CSM, which essentially expressed its disagreement with the composition

[60] See Montoro, *Uso y cesión de datos de carácter personal en el proceso penal...*, 840.

[61] On the legislative path in Portugal and the current situation on the matter in question, see Wengorovius, "Tribunais e Regulamento (UE) 2016/679...", 471-774.

[62] The complete parliamentary activity in relation to this Bill, until its veto by the President of the Portuguese Republic and subsequent expiry of the Bill, can be consulted on the website of the *Assembleia da República* at: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42506.

of the *Comissão para a Coordenação da Gestão dos Dados Referentes ao Sistema Judicial*. We will, however, discuss this report in relation to Article 23(1)(a) of the aforementioned Bill. The Bill proposed the amendment in the sense that it should be the Judges and Magistrates of the Public Prosecutor's Office competent in their corresponding activities who should hold the status of "*controllers*", [according to the definition contained in Article 3(8) GDPR]. The CSM issued a report[63] opposing the particular question on the judges and courts as data "*controllers*" by stating that "*The judicial activity of judges relating to the processing of personal data in court proceedings, for the purposes of the Regulation, is not assimilable to the notion of «controller» as defined in the GDPR*"[64] and also that *"The jurisdictional activity of judges regarding the processing of personal data in court proceedings does not determine either the means (made available to and managed by the Ministry of Justice) or the purposes (established by law)*."[65]

Let us recall that the current situation in relation to the status of the "*controller*"[66] in the courts in Portuguese the legal regime is as follows: the responsibility for data processing corresponds to the "*responsáveis pela gestão dos dados"* [management of data] whose competences are exercised in a coordinated manner through the *Comissão para a Coordenação da Gestão dos Dados Referentes ao Sistema Judicial*. The CSM *"is the entity responsible for the management of data relating to: the proceedings in the judicial courts; the measures of coercion deprivation of liberty and detention; the procedural connection in criminal proceedings when the connection operates in relation to proceedings that are simultaneously in the investigation or trial phase; and the arrest warrants when the arrest warrant is issued by the judge (articles 24 (1), a), b) and c) and (3), a), e), g) and h) [Law 34/2009, of 14 July]; the Conselho Superior dos Tribunais Administrativos e Fiscais (CSTAF) is the entity responsible for the management of data contained in the files of the administrative and tax courts (Article 24 (2), (3) b) [Law 34/2009, of 14 July] (...). And according to Article 24(6) of Law 34/2009, of 14 July, it is the responsibility of those responsible for data management*:

> *a) Ensure the legality of consultation and communication of information;*
> *b) Guarantee the fulfilment of measures necessary for the security of information and data processing;*
> *c) Ensuring compliance with the access and security rules for the electronic archive.*
> *Being guaranteed by the Magistrates with competence on the respective procedure, according to the terms of number 7 of the aforementioned law the following:*
> *a) The right of information and the right of access to data by the respective owner;*
> *b) Updating data, correcting any that are inaccurate, filling in any that are totally or partially missing and deleting any that are unduly recorded.*
> *c) The other competences provided for in the Personal Data Protection Act (...)*."[67]

In our opinion, and in line with the position we have been defending throughout this paper, based on the characteristics and functions of the *"controller"*, it should be the judges and courts themselves who should have this status of data *"controller"*, as provided for in Article 23(1)[68] of the aforementioned Bill. The

[63] The full CSM Report can be found on the website of the *Assembleia da República* on the above-mentioned link.

[64] Report issued by the *Conselho Superior da Magistratura (CSM)* on the *Second Amendment to Law 34/2009, of 14 July, on the legal regime applicable to the processing of data concerning the judicial system*, 4."

[65] Report issued by the *Conselho Superior da Magistratura (CSM)* on the *Second Amendment to Law 34/2009, of 14 July, on the legal regime applicable to the processing of data concerning the judicial system*, 5."

[66] "*Responsável pelo tratamento"* as is defined in the Portuguese translation of the GDPR in Article 4(7).

[67] See Wengorovius, "Tribunais e Regulamento (UE) 2016/679...", 458.

[68] "*Article 23 (...) For the purposes of the personal data protection regimes, the following are [data] controllers: a)*

reason for the attribution to judges and courts of the status of "*controller*", as has already been pointed out in this paper, is to be found in the fact that since the purpose and the means of processing personal data in the exercise of the judicial function are established by law, it is arguable that *"the law or the Constitution itself have also established that courts are the «controller» of personal data processed in the context of the exercise of the judicial function, as courts must process personal data for that purpose, and the judicial function remains theirs and theirs alone*."[69] The basis for this reasoning, is also to be found, as was also mentioned above, in the GDPR, specifically in Recital (20) when it states: "*While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities*." Also in Article 4(7) on the definition of "*controller*" when it states *in fine* that: *"where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*" and finally in Article 26(1) GDPR *in fine: "the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject*."[70]

We also understand in this sense that the aforementioned report of the *Conselho Superior da Magistratur*a (CSM),[71] when it states that "*The jurisdictional activity of judges regarding the processing of personal data in court proceedings does not determine either the means (made available to and managed by the Ministry of Justice) nor the purposes (established by law)*",[72] does not take into account (as we mentioned when discussing the Spanish legislation and the LexNet system managed by the Spanish Ministry of Justice) that the Services of the Portuguese Ministry of Justice would have in this case the status of "*processor*" [*Subcontratante*] or "*joint controller*" [*Responsáveis conjuntos pelo tratamento*] according to the competences laid down by

Judicial magistrates and public prosecutors competent under the terms of the procedure law, with regard to data processed within the scope and acts of the procedure, in the exercise of their procedural activity and under their direction or authority; (...)." Also, the expression *"Under the terms of the procedure law"*, as was pointed out by José Luís Lopes da Mota *"would also oblige to examine the need to amend the procedural laws currently in force so that judges and tribunals could assume the competence as «Controllers» [«Responsáveis pelo tratamento»]*."

[69] Giacomo Bonetto, "Data protection and the exercise of the judicial function in Ireland", *Irish Judicial Studies Journal*, vol. 4(2), (2020): 72.

[70] See, Article 202 (1)(2) of the Portuguese Constitution: "*Jurisdictional function 1. The courts are the entities that exercise sovereignty with the competence to administer justice in the name of the people. 2. In administering justice, the courts are responsible for ensuring the defence of those citizens' rights and interests that are protected by law, repressing breaches of democratic legality and deciding conflicts between interests, public and private*"; Article 203 of the Portuguese Constitution: "*(Independence). The courts are independent and subject only to the law";* see also the Portuguese Law 62/2013, of 26 August, on the organisation of the judiciary, Article 2: *"Courts and Jurisdictional function*", Article 4: "*Independence of the Judges*" and Article 22: "*Independence of the Courts*"); and finally, see Portuguese Law 21/85, of 30 July on the Statute of Judicial Magistrates, Article 3: "*Function of the Judiciary*" and Article 4: "*Judicial Independence.*"

[71] Wengorovius also agrees with the CMS report in the criticism of Article 23 of the vetoed Bill in this sense:"*The jurisdictional activity of judges regarding the processing of personal data in court proceedings, is not assimilable to the notion of «controller» as defined in the GDPR. The Judge or the Public Prosecutor do not determine either the means made available by the Ministry of Justice (IGFEJ, I.P.), nor the purposes, which are laid down in Article 4 of Law 34/2009 and in the procedural laws."* Wengorovius, "Tribunais e Regulamento (UE) 2016/679...", 473. The original citation is in Portuguese.

[72] The original citation in Portuguese reads: "*A atividade jurisdicional dos juízes relativa ao tratamento de dados pessoais nos processos judiciais não determina nem os meios (colocados à disposição e geridos pelo Ministério da Justiça) nem as finalidades (estabelecidas pela lei).*"

law[73] not entering into collision at any time with the judge or court that would have the status of "*controller*" [*Responsável pelo tratamento*] with different functions (being reserved to the judges the protection of the rights of the data subject).[74]

We would then return to the distinction made by Montoro and already commented in the previous point on the *"formal"* dimension of data processing (held by the judge or court as "*controller*") and the *"material"* dimension (who would have the status of "*processor*" or eventually the status of "*joint controller*" according to the competences and responsibilities laid down by law).[75]

5. Conclusion

After analysing the functions of the "*controller*", and in particular its characteristics and its role in the courts, having paid special attention to the legislative framework currently in force in Portugal and Spain, we can draw the following conclusions:

The formal status of the "*controller*" within the judicial system must be held by each of the judges and courts, acting in judicial capacity in the context of individual

---

[73] See, in this sense, Articles 23, 24 and 26 of the Portuguese Law (in force) 34/2009, of 14 July, which establishes the legal regime applicable to the processing of data relating to the judicial system, Article 23: "*Data Controllers. For the purposes of the [Portuguese] Personal Data Protection Act, approved by Act 67/98 of 26 October, the role of Data Controller provided for in the present law is incumbent on: a) Those responsible for data management, whose competences are exercised in a coordinated manner through the Commission for the Coordination of Data Management regarding the Judicial System, provided for in this chapter; b) Those magistrates with jurisdiction over the respective procedure, under the terms of the law*"; Article 24: "*Data Controllers Entities*", see, particularly 24 (7): "*The magistrates with jurisdiction over the respective procedure, the justices of the peace responsible for the procedures or the mediators involved in the mediation process, depending on the case, shall ensure: a) The right to information and the right of access to data by the respective data subject; b) The updating of data, as well as the correction of inaccurate data, the completion of any that are totally or partially missing and the deletion of any that are unduly recorded. c) The other powers provided for in the Portuguese Personal Data Protection Act, approved by Law 67/98 of 26 October*"; and Article 26: "*Application development. 1. The Ministry of Justice shall ensure, through the department with competence for the matter in question, without prejudice to the regimes of judicial secrecy and State secrecy, the development of the computer applications necessary for the processing of procedures and the management of the judicial system, including the necessary analysis, implementation and support. 2. The development of computer applications for the processing of data relating to the judicial system shall take into account the use of non-proprietary applications and the adoption of open standards for information in digital format*". See also, Portuguese Decree Law no. 123/2011, of 29 December approving the Organic Law of the Ministry of Justice, article 11(1): "*Directorate-General for the Administration of Justice 1. The mission of the Directorate-General for the Administration of Justice, abbreviated to DGAJ, is to ensure support for the functioning of the courts*", and Article 14 (1): "*Institute for the Financial Management and Equipment of Justice, I. P. (1) The mission of the Institute for the Financial Management and Equipment of Justice I. P., abbreviated to IGFEJ, I. P., is to manage the financial resources of the Ministry of Justice, to manage the assets allocated to the area of justice, infrastructures and technological resources, as well as to propose the design, implementation and evaluation of computerisation plans and projects, in conjunction with the other services and bodies of the Ministry of Justice.*" Finally, see Articles 136 and 139 (Competences of the CSM) of the Portuguese Law no. 21/85 of 30 July (Statute of Judicial Magistrates). Please note that Portuguese Law 67/98 of 26 October was replaced by GDPR.

[74] See Articles 12 to 18 GDPR.

[75] Also, in the aforementioned Portuguese vetoed Bill the following was foreseen in this regard. The original citation in Portuguese reads: "*Artigo 25.º Comissão de Coordenação da Gestão da Informação do Sistema Judiciário. 1 - As competências das entidades supervisoras da gestão da informação são exercidas diretamente ou em cooperação e de forma coordenada através da Comissão de Coordenação da Gestão da Informação do Sistema Judiciário, adiante designada por Comissão. 2 - A Comissão é constituída pelo conselho superior e pelo conselho coordenador . 3 - Compete à Comissão: a) Assegurar o exercício coordenado das competências das entidades supervisoras da gestão da informação, nomeadamente a adoção das medidas técnicas e organizativas adequadas a garantir a segurança dos dados pessoais; (...).*"

cases as well in the judicial activity, as recently defined in the CJEU judgment of 24 March 2022 in case C-245/20 "*in the sense that it is not limited to the processing of personal data carried out by courts in the context of individual cases, but refers more broadly to all processing operations carried out by courts in the context of their judicial activity, with the result that processing operations whose control by the supervisory authority could directly or indirectly influence the independence of its members or weigh on their decisions are excluded from the competence of the supervisory authority*", all with the aim of preserving the independence and impartiality of the judiciary in the exercise of their functions by avoiding any possible interference in this regard by the supervisory authority.

We consider necessary to resume as a priority the legislative activity in Portugal in the sense of amending the legal regime applicable to the processing of data referring to the judicial system, following the veto of 29 July 2019 by the President of the Portuguese Republic and the expiry of the Bill that sought to amend Law 34/2009, in order to bring the Law still in force into line with the provisions contained in the GDPR.

In this sense, we consider, as we have already made clear before, that in the Portuguese legislation the status of "*controller*" ["*Responsável pelo tratamento*"] should be held by the judge and the courts of each jurisdiction, in line with what was proposed in the amendment to Article 23 of the vetoed Bill mentioned above. This would mean that the *Conselhos Superiores* (CSM and CSTAF) would not hold the status of "*controllers*" for "*jurisdictional purposes*." This is consistent with the strict respect for the principle of independence of the judiciary and the natural attribution of the status of (data) "*controller*" to the judge or court before which the proceedings are being conducted and which also carries out data processing operations for jurisdictional purposes.

This criterion has been ratified in Spain by the 3rd Chamber of the Supreme Court in its Sentence 1611/2018 of 13 November, which clearly establishes that the status of "*controller*" ["*Responsável pelo tratamento*"] is held by each judge or court individually, rejecting that the General Council of the Judiciary (CGPJ), [*Consejo General del Poder Judicial*], can hold such a position or perform the functions inherent to it.

The role and the competences of the "*controller*" in the courts must be perfectly delimited, in order to guarantee an effective implementation of its tasks and the exercise of the data subject's rights. In this sense, and in line with the Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of «controller» and «processor»*, 00264/10/EN WP 169, adopted on 16 February 2010,[76] "*If it is not sufficiently clear what is required and from whom – for example, no one is responsible or there are several possible controllers – there is a clear risk that little or nothing happens and the legal provisions will be ineffective*."

Article received on 4 December 2024 and accepted for publication on 19 January 2025.

[76] See pages 7 and 8.