SUPREMO TRIBUNAL DE JUSTIÇA

PORTUGUESE JURISPRUDENCE

PERSONAL DATA PROTECTION

REGULATION (EU) 2016/679, OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016

LAW NO. 58/2019, OF 08.08

JANUARY 2023 TO DECEMBER 2023

COMPILED BY:

CÁTIA COSTA SANTOS

(JUDGE ADVISOR OF THE SUPREME COURT OF JUSTICE)

I. CONSTITUTIONAL COURT

- **Judgement of the Constitutional Court no. 91/2023**
  Rapporteur: Councillor Joana Fernandes da Costa

"*DECISION:*

In light of the foregoing, the Constitutional Court decides:

(a) To decline to consider the subject matter of the appeal concerning the provision inferred from Articles 8, 17, 18, 20, and 67(1)(h) and (f) of the Legal Framework for Competition, in the version approved by Law no. 19/2012, of 8 May, which stipulates that, in an investigation opened for restrictive competition practices, searches and seizures can be conducted without suspicion of specific facts constituting an infringement;

(b) Not to declare unconstitutional the provision contained in Article 18(1)(c) of the Legal Framework for Competition, in the version approved by Law no. 19/2012, of 8 May, which allows the Competition Authority to search and seize email messages marked as opened in administrative offence proceedings for restrictive competition practices, with judicial authorisation;

(c) To declare unconstitutional, for violation of the provisions of Articles 32(4) and 34(1) and (4), the latter in conjunction with Article 18(2), all of the Constitution, the provision derived from the combined provisions of Article 18(2) and Article 20(1) of the Legal Framework for Competition, in the version approved by Law no. 19/2012, of 8 May, which allows the Competition Authority to search and seize opened email messages with the authorisation of the Public Prosecutor's Office in administrative offence proceedings for restrictive competition practices; and, consequently,

(d) To partially grant the appeal, ordering the amendment of the appealed decision in accordance with the positive judgement of unconstitutionality expressed in paragraph (c).'

https://www.tribunalconstitucional.pt/tc/acordaos/20230091.html

- **Judgement of the Constitutional Court no. 240/2023**
  Rapporteur: Councillor José António Teles Pereira

"*Decision*
In light of the foregoing, it is decided:
(a) Not to declare unconstitutional the normative interpretation of Article 8(2) of Law no. 5/2008, according to which it is possible to collect DNA samples from defendants convicted to a specific term of imprisonment equal to or greater than 3 years, even if substituted.
(b) Consequently, to dismiss the appeal.'
https://www.tribunalconstitucional.pt/tc/acordaos/20230240.html

- **Judgement of the Constitutional Court no. 314/2023**
  Rapporteur: Councillor José António Teles Pereira

"*Decision*
3. In light of the foregoing, it is decided:
(a) To declare unconstitutional the provision contained in Articles 18(1)(c)(2), 20(1), and 21 of the New Legal Framework for Competition, approved by Law no. 19/2012, of 8 May, in the interpretation according to which the examination, collection, and seizure of emails in competition offence proceedings are allowed, provided it is authorised by the Public Prosecutor's Office, without the need for prior judicial approval, for violation of the provisions of Articles 32(4) and 34(1) and (4), the latter in conjunction with Article 18(2), all of the Constitution; and, consequently,
(b) To grant the appeal, ordering the referral of the case to the Lisbon Court of Appeal for it to amend the decision in accordance with the unconstitutionality declared herein."
https://www.tribunalconstitucional.pt/tc/acordaos/20230314.html

II. SUPREME COURT OF JUSTICE

- **Judgement of the Supreme Court of Justice of 13-04-2023**
  Case: no. 4778/11.8JFLSB-B.S1- 3rd Section
  Rapporteur: Councillor Lopes da Mota

I. In accordance with Article 449(1)(f) of the CPP, the revision of a final judgement is admissible when the Constitutional Court (TC) declares the unconstitutionality, with general binding force, of a provision less favourable to the defendant that served as the basis for the conviction.
II. Requiring an interpretation in accordance with the Constitution, the content of the provision is narrowly limited, in conjunction with Article 282(3) of the Basic Law: a revision can only occur on this basis, assuming that such a provision has a penal nature less favourable to the accused, when the Constitutional Court (TC) issues a decision contrary to the reservation imposed by the constitutionally final judgement; in the absence of a decision to the contrary, all final judgements that have applied the provision declared unconstitutional remain unaffected.
III. The provisions of Law no. 32/2008, of 17 July, which the TC declared unconstitutional, with general binding force, in judgement no. 268/2022, relate to the retention, for a period of one year, by providers of publicly available electronic communications services or of a public communications network, of traffic and location data relating to natural and legal persons, as well as the associated data necessary for identifying the subscriber or registered user, for the purposes of investigating, detecting, and prosecuting serious crimes, as defined in the domestic law of each Member State, by the competent national authorities.
IV. Law no. 32/2008 transposes into the domestic legal system Directive no. 2006/24/EC, of 15 March, amending Directive no. 2002/58/EC, of 12 June, adopted under Article 95 of the Treaty establishing the European Community (pertaining to the functioning of the internal market, the former 1st pillar of the Union), the main aim of which was to harmonise the provisions of the Member States concerning the obligations of providers

of electronic communications services or public communications networks to retain such data, in derogation of Articles 5, 6, and 9 of Directive 2002/58/EC, which transposed the principles laid down in Directive 95/46/EC (transposed into domestic law by Law no. 67/98, of 26 October, subsequently replaced by the GDPR) into specific rules for the electronic communications sector.

V. Article 15(1) of Directive 2002/58/EC, transposed into domestic law by Law no. 41/2004 of 18 August, provides that, for this purpose, Member States may adopt legislative measures and lists the conditions for restricting confidentiality and prohibiting the storage of traffic and location data, but does not apply to the activities of the State in criminal law matters, which constituted a domain of intergovernmental cooperation (former 3rd pillar of the Union).

VI. Always needing to distinguish between data retention activities, regulated by 'Community law' provisions (former 1st pillar), and data access activities, regulated by domestic criminal procedural provisions and the former third pillar of the Union (a distinction that must be maintained after the Treaty of Lisbon, with the abolition of the 'pillarisation' of Maastricht), which constitute different personal data processing operations and, as such, distinct interferences with fundamental rights, it is the responsibility of domestic law to determine the conditions under which service providers must grant access to data to competent national authorities (interference with the right to privacy) for the investigation of serious crime, respecting the principles and rules of criminal procedure, including the principles of proportionality, prior judicial oversight, adversarial proceedings, and equitable process (see judgements of the CJEU of 21.12.2016, Tele2 Sverige AB, Case C-203/15; 6.10.2020, La Quadrature du Net and others, Cases C-511/18, C-512/18, and C-520/18; 2.3.2021, H. K. and Prokuratuur, Case C-746/18; and of 5.4.2022, G. D. and Commissioner of An Garda Síochána and others, Case C-140/20).

VII. Access to personal data by competent authorities for the purposes of preventing, investigating, detecting, or prosecuting criminal offences or enforcing criminal sanctions, which adheres to these rules and principles, is currently governed by Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities in the framework of criminal

investigations and prosecutions, transposed into domestic law by Law no. 59/2019, of 08 August (see Articles 1 and 2(1)).

VIII. In a different dimension, Law no. 32/2008 neither repealed nor established rules of a penal or criminal procedural nature, from which judicial authorities should seek assistance for access and acquisition of evidence or to ensure its validity in the proceedings; such activities are subject to their own framework defined by domestic criminal and criminal procedural laws and, with regard to the areas of competence of the European Union (EU) within the space of freedom, security, and justice - which is a competence shared between the EU and the Member States (Article 5(2) of the Treaty on the Functioning of the European Union - TFEU) - by Article 82 of the TFEU and the aforementioned Directive (EU) 2016/680 of the European Parliament and of the Council, transposed by Law no. 59/2019, of 8 August.

IX. The obtaining of data from communication service providers in criminal proceedings is regulated by other legal provisions: by Articles 187 to 189 and 269(1)(e) of the CPP and by Law no. 109/2009, of 15 September (Cybercrime Law), which transposes into the domestic legal system Framework Decision no. 2005/222/JHA of 24 February on attacks against information systems, and aligns domestic law with the Council of Europe Convention on Cybercrime (Budapest, 2001); RAR no. 88/2009 and DPR no. 91/2009, of 15 September).

X. The Constitutional Court did not declare that the effects of the declaration of unconstitutionality with general binding force, as per judgement no. 268/2022, extend to res judicata, in accordance with Article 282(3) of the Constitution, so this declaration of unconstitutionality does not constitute grounds for the revision of a judgement under article 449(1)(f) of the CPP.

XI. The declaration of invalidity of Directive no. 2006/24/EC by the Court of Justice of the European Union (CJEU), by judgement of 08.04.2014, in preliminary ruling requests submitted under Article 267 of the TFEU (in the joined cases Digital Rights Ireland Ltd (C-293/12) and Kärntner Landesregierung (C-594/12), pre-dating the judgement under which the appellant was convicted, does not constitute grounds for revision of the judgement referred to in Article 449(1)(g) of the CPP, according to which a revision is admissible when 'a binding judgement of the Portuguese State, issued by an international instance, is incompatible with the conviction or raises serious doubts about its fairness.'

XII. In addition to the law requiring that the judgement rendered by an international instance be subsequent to the conviction, the judgement of the CJEU – not the European Court of Human Rights, for which the provision was particularly designed, considering Article 46(1) (under the heading 'Binding force and execution of judgements') of the European Convention on Human Rights – does not constitute 'a binding judgement' of the Portuguese State within the meaning of this provision.
XIII. A judgement of the CJEU that, in a preliminary appeal, declares a directive invalid under Article 267 of TFEU, is addressed directly to the judicial body that referred the matter to the CJEU; the fact that any other judicial body must consider such an act invalid due to the general obligation to ensure the primacy of Union law, refraining from acts contrary to it that might impair its effectiveness (in this sense, one can speak of an erga omnes effectiveness – see CJEU judgement C-66/80 of 13 May, 1981), does not confer upon it the status of a party directly affected by that decision, so it should not be considered as a binding judgement serving as a ground for revision.
XIV. Thus, as there are no grounds, the revision of the judgement is denied.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:STJ:2023:4778.11.8JFLSB.B.S1.1A/

- **Judgement of the Supreme Court of Justice of 13-04-2023**
  Case: no. 104/21.6JAVRL.C1.S1- 3rd Section
  Rapporteur: Councillor Orlando Gonçalves

I - Nullity for failure to rule, provided for in Article 379(1)(c) of the CPP, occurs when the court fails to rule on issues raised or known of its own motion that are not prejudiced by the solution given to others.
II - Given that the Court of Appeal addressed, in the appealed judgement, the issue submitted to its consideration according to the terms defined by the appellant, the nullity of the judgement for failure to rule is not established.
III - The declaration of unconstitutionality handed down in judgement no. 268/2022 encompasses evidence collected and stored regarding communications made or attempted, excluding from its scope telephone interceptions, which are regulated in Article 187 of the CPP, and the respective content data obtained in real time.

IV - Not only do real-time traffic and location data fall outside the scope of Law no. 32/2008, but also basic data when inherent to telephone interceptions.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:STJ:2023:104.21.6JAVRL.C1.S1.AD/

- **Judgement of the Supreme Court of Justice of 04-05-2023**
  Case: no. 16/18.0GAOAZ-D.S1- 3rd Section
  Rapporteur: Councillor Lopes da Mota

I. In accordance with Article 449(1)(f) of the CPP, the revision of a final judgement is admissible when the Constitutional Court (TC) declares the unconstitutionality, with general binding force, of a provision less favourable to the defendant that served as the basis for the conviction.
II. In an interpretation in accordance with the Constitution, the content of the provision is narrowly limited, in conjunction with Article 282(3) of the Basic Law: a revision can only occur on this basis, assuming that such a provision has a penal nature less favourable to the accused, when the Constitutional Court (TC) issues a decision contrary to the reservation imposed by the constitutionally final judgement; in the absence of a decision to the contrary, all final judgements that have applied the provision declared unconstitutional remain unaffected.
III. The provisions of Law no. 32/2008, of 17 July, which the TC declared unconstitutional, with general binding force, in judgement no. 268/2022, relate to the retention by providers of publicly available electronic communications services or of a public communications network, of traffic and location data relating to natural and legal persons, as well as the associated data necessary for identifying the subscriber or registered user, for the purposes of investigating, detecting, and prosecuting serious crimes, as defined in the domestic law, by the competent national authorities.
IV. The data processed and stored are data pertain to communications in their various forms, with each record beginning with the establishment of communication and ending with its termination; data which, although they may be identical, have not been processed in relation to communications made (for example, data relating to the identification of subscribers obtained and processed within the framework of the contractual relationship with the service provider) are excluded.

V. Law no. 32/2008 transposes into the domestic legal system Directive no. 2006/24/EC, of 15 March, amending Directive no. 2002/58/EC, of 12 June, adopted under Article 95 of the Treaty establishing the European Community (pertaining to the functioning of the internal market, the former 1st pillar of the Union), the main aim of which was to harmonise the provisions of the Member States concerning the obligations of providers of electronic communications services or public communications networks to retain such data, in derogation of Articles 5, 6, and 9 of Directive 2002/58/EC, which transposed the principles laid down in Directive 95/46/EC (transposed into domestic law by Law no. 67/98, of 26 October, subsequently replaced by the GDPR) into specific rules for the electronic communications sector.

V. Article 15(1) of Directive 2002/58/EC, transposed into domestic law by Law no. 41/2004 of 18 August, provides that, for this purpose, Member States may adopt legislative measures and lists the conditions for restricting confidentiality and prohibiting the storage of traffic and location data, but does not apply to the activities of the State in criminal law matters, which constituted a domain of intergovernmental cooperation (former 3rd pillar of the Union).

VII. A distinction must be made between data retention operations, regulated by 'Community law' provisions (former 1st pillar), and data access operations, regulated by domestic criminal procedural provisions and the former 3rd pillar of the Union (a distinction that must be maintained after the Treaty of Lisbon, with the abolition of the 'pillarisation' of Maastricht), which constitute different personal data processing operations and, as such, distinct and autonomous interferences with fundamental rights - in this case, the right to privacy, including the right to the protection of personal data, which, safeguarding the principles, admit restrictions necessary for the protection of other rights, in particular the right to freedom and security.

VIII. It is the responsibility of domestic law to determine the conditions under which service providers must grant access to data to competent national authorities (interference with the right to privacy) for the investigation of serious crime, respecting the principles and rules of criminal procedure, including the principles of proportionality, prior judicial oversight, adversarial proceedings, and equitable process (see judgements of the CJEU of 21.12.2016, Tele2 Sverige AB, Case C-203/15; 6.10.2020, La Quadrature du Net and others, Cases C-511/18, C-512/18, and C-520/18; 2.3.2021, H. K. and Prokuratuur, Case

C-746/18; and of 5.4.2022, G. D. and Commissioner of An Garda Síochána and others, Case C-140/20).

IX. Access to personal data by competent authorities, as a data processing operation for the purposes of preventing, investigating, detecting, or prosecuting criminal offences, which complies with these rules and principles, is currently governed by Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities in the framework of criminal investigations and proceedings, transposed into domestic law by Law no. 59/2019, of 8 August.

X. Considering that data retention for the purposes of criminal investigation, particularly for serious crimes as defined by domestic law, is allowed by Article 15(1) of Directive 2002/58/EC (and in Law 41/2004, which transposes it), Directive 2006/24/EC aimed, given the significant disparities in domestic laws causing practical difficulties and impeding the functioning of the internal market, to establish harmonisation norms within the European Union space for the retention of traffic data, location data, and related data - norms that determine the purpose of data processing (adhesion to the principle of purpose, a fundamental principle that, along with the principles of legality, necessity, and proportionality, govern the processing of personal data) - but did not regulate, nor could it regulate, the activity of public authorities (criminal police and judicial authorities – Public Prosecutor's Office, judges, and courts) with competence to ensure the achievement of that purpose through criminal proceedings.

XI. In a different dimension, Law no. 32/2008 neither repealed nor established rules of a penal or criminal procedural nature, from which judicial authorities should seek assistance for access and acquisition of evidence or to ensure its validity in the proceedings; such activities are subject to their own framework defined by domestic criminal and criminal procedural laws and, with regard to the areas of competence of the European Union (EU) within the space of freedom, security, and justice - which is a competence shared between the EU and the Member States (Article 5(2) of the Treaty on the Functioning of the European Union - TFEU) - by Article 82 of the TFEU and Directive (EU) 2016/680 of the European Parliament and of the Council, transposed by Law no. 59/2019, of 8 August.

XII. The obtaining of data from communication service providers in criminal proceedings is regulated by other legal provisions: by Articles 187 to 189 and 269(1)(e) of the CPP and by Law no. 109/2009, of 15 September (Cybercrime Law), which transposes into the domestic legal system Framework Decision no. 2005/222/JHA of 24 February on attacks against information systems, and aligns domestic law with the Council of Europe Convention on Cybercrime (Budapest, 2001), ratified by Portugal.

XIII. The Constitutional Court did not declare that the effects of the declaration of unconstitutionality with general binding force, as per judgement no. 268/2022, extend to res judicata, in accordance with Article 282(3) of the Constitution, so this declaration of unconstitutionality does not constitute grounds for the revision of a judgement under article 449(1)(f) of the CPP.

XIV. The declaration of invalidity of Directive no. 2006/24/EC by the Court of Justice of the European Union (CJEU), by judgement of 08.04.2014, in preliminary ruling requests submitted under Article 267 of the TFEU (in the joined cases Digital Rights Ireland Ltd (C-293/12) and Kärntner Landesregierung (C-594/12), pre-dating the judgement under which the appellant was convicted, does not constitute grounds for revision of the judgement referred to in Article 449(1)(g) of the CPP, according to which a revision is admissible when 'a binding judgement of the Portuguese State, issued by an international instance, is incompatible with the conviction or raises serious doubts about its fairness.'

XV. In addition to the law requiring that the judgement rendered by an international instance be subsequent to the conviction, the judgement of the CJEU does not constitute 'a binding judgement' on the Portuguese State, within the meaning of this provision, which was designed for the decisions of the European Court of Human Rights (considering Article 46(1) of the ECHR).

XVI. A judgement of the CJEU that, in a preliminary appeal, declares a directive invalid under Article 267 of TFEU, is addressed directly to the judicial body that referred the matter to the CJEU; the fact that the CJEU's decision constitutes sufficient reason for any other judicial body to consider such an act invalid due to the general obligation to ensure the primacy of Union law, refraining from acts contrary to it that might impair its effectiveness (in this sense, one can speak of an erga omnes effectiveness – see CJEU judgement C-66/80 of 13 May, 1981), does not confer upon it the status of a party directly

affected by that decision, so it should not be considered as a binding judgement serving as a ground for revision.

XVII. Thus, as there are no grounds, the revision of the judgement is denied.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:STJ:2023:16.18.0GAOAZ.D.S1.9D/

- **Judgement of the Supreme Court of Justice of 13-04-2023**
  Case: no. 1570/18.2T8TMR-B.L1.S2- 4th Section
  Rapporteur: Councillor Ramalho Pinto

Exceptional revision is admissible in a case where, while discussing the unlawfulness of the dismissal of the Plaintiff based on the inadequacy of the justifying reason for collective dismissal, issues of significant complexity are being debated, involving, in order to determine whether the dismissal decision allows one to perceive and scrutinise why the Plaintiff was selected, her evaluation compared to that of other employees. Additionally, indicating the evaluation of these other employees may entail a violation of the General Data Protection Regulation.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:STJ:2023:1570.18.2T8TMR.B.L1.S2.19/

- **Judgement of the Supreme Court of Justice of 13-09-2023**
  Case: no. 1570/18.2T8TMR-B.L1.S1- 4th Section
  Rapporteur: Councillor Domingos José de Morais

I - The decision to carry out a collective dismissal that excluded a specific employee due to a lower performance evaluation should include the objective criteria for the performance evaluation of comparable employees, so that the court can assess and decide on the grounds for the dismissal of that employee.

II - The prohibition on processing personal data as stipulated in Article 9(1) of the General Data Protection Regulation of the European Union is excepted if the processing is necessary for the defence of a right in legal proceedings or where the courts are acting in the exercise of their judicial function;

III - Given that the Constitution of the Portuguese Republic prohibits dismissals without just cause or for political or ideological reasons, the exception to the prohibition on processing personal data in the context of a legal challenge to dismissal is justified.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:STJ:2023:1570.18.2T8TMR.B.L1.S1.A5/

- **Judgement of the Supreme Court of Justice of 19-12-2023**
  Case: no. 191/17.1JELSB-K.S1- 3rd Section
  Rapporteur: Councillor Lopes da Mota

I. In accordance with Article 449(1)(f) of the CPP, the revision of a final judgement is admissible when the Constitutional Court ('TC') declares the unconstitutionality, with general binding force, of a provision less favourable to the defendant that served as the basis for the conviction.
II. In an interpretation in accordance with the Constitution, Article 282(3) a revision can only occur on this basis, assuming that such a provision has a penal nature less favourable to the accused, when the Constitutional Court (TC) issues a decision contrary to the reservation imposed by the constitutionally final judgement; in the absence of a decision to the contrary, all final judgements that have applied the provision declared unconstitutional remain unaffected.
III. The provisions of Law no. 32/2008, of 17 July, which the TC declared unconstitutional, with general binding force, in judgement no. 268/2022, relate to the retention by providers of publicly available electronic communications services or of a public communications network, of traffic and location data relating to natural and legal persons, as well as the associated data necessary for identifying the subscriber or registered user, for the purposes of investigating, detecting, and prosecuting serious crimes, as defined in the domestic law, by the competent national authorities.
IV. The data processed and stored are data pertain to communications in their various forms, with each record beginning with the establishment of communication and ending with its termination; data which, although they may be identical, have not been processed in relation to communications made (for example, data relating to the identification of

subscribers obtained and processed within the framework of the contractual relationship with the service provider) are excluded.

V. Law no. 32/2008 transposes into the domestic legal system Directive no. 2006/24/EC, of 15 March, amending Directive no. 2002/58/EC, of 12 June, adopted under Article 95 of the Treaty establishing the European Community (pertaining to the functioning of the internal market, the former 1st pillar of the Union), the main aim of which was to harmonise the provisions of the Member States concerning the obligations of providers of electronic communications services or public communications networks to retain such data, in derogation of Articles 5, 6, and 9 of Directive 2002/58/EC, which transposed the principles laid down in Directive 95/46/EC (transposed into domestic law by Law no. 67/98, of 26 October, subsequently replaced by the GDPR) into specific rules for the electronic communications sector.

V. Article 15(1) of Directive 2002/58/EC, transposed into domestic law by Law no. 41/2004 of 18 August, provides that, for this purpose, Member States may adopt legislative measures and lists the conditions for restricting confidentiality and prohibiting the storage of traffic and location data, but does not apply to the activities of the State in criminal law matters, which constituted a domain of intergovernmental cooperation (former 3rd pillar of the Union).

VII. A distinction must be made between data retention operations, regulated by 'Community law' provisions (former 1st pillar), and data access operations, regulated by domestic criminal procedural provisions and the former 3rd pillar of the Union (a distinction that must be maintained after the Treaty of Lisbon, with the abolition of the 'pillarisation' of Maastricht), which constitute different personal data processing operations and, as such, distinct and autonomous interferences with fundamental rights - in this case, the right to privacy, including the right to the protection of personal data, which, safeguarding the principles, admit restrictions necessary for the protection of other rights, in particular the right to freedom and security.

VIII. It is the responsibility of domestic law to determine the conditions under which service providers must grant access to data to competent national authorities (interference with the right to privacy) for the investigation of serious crime, respecting the principles and rules of criminal procedure, including the principles of proportionality, prior judicial oversight, adversarial proceedings, and equitable process (see judgements of the CJEU of

21.12.2016, Tele2 Sverige AB, Case C-203/15; 6.10.2020, La Quadrature du Net and others, Cases C-511/18, C-512/18, and C-520/18; 2.3.2021, H. K. and Prokuratuur, Case C-746/18; and of 5.4.2022, G. D. and Commissioner of An Garda Síochána and others, Case C-140/20).

IX. Access to personal data by competent authorities, as a data processing operation for the purposes of preventing, investigating, detecting, or prosecuting criminal offences, which complies with these rules and principles, is currently governed by Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities in the framework of criminal investigations and proceedings, transposed into domestic law by Law no. 59/2019, of 8 August.

X. Considering that data retention for the purposes of criminal investigation, particularly for serious crimes as defined by domestic law, is allowed by Article 15(1) of Directive 2002/58/EC (and in Law 41/2004, which transposes it), Directive 2006/24/EC aimed, given the significant disparities in domestic laws causing practical difficulties and impeding the functioning of the internal market, to establish harmonisation norms within the European Union space for the retention of traffic data, location data, and related data - norms that determine the purpose of data processing (adhesion to the principle of purpose, a fundamental principle that, along with the principles of legality, necessity, and proportionality, govern the processing of personal data) - but did not regulate, nor could it regulate, the activity of public authorities (criminal police and judicial authorities – Public Prosecutor's Office, judges, and courts) with competence to ensure the achievement of that purpose through criminal proceedings.

XI. In a different dimension, Law no. 32/2008 neither repealed nor established rules of a penal or criminal procedural nature, from which judicial authorities should seek assistance for access and acquisition of evidence or to ensure its validity in the proceedings; such activities are subject to their own framework defined by domestic criminal and criminal procedural laws and, with regard to the areas of competence of the European Union (EU) within the space of freedom, security, and justice - which is a competence shared between the EU and the Member States (Article 5(2) of the Treaty on the Functioning of the European Union - TFEU) - by Article 82 of the TFEU and

Directive (EU) 2016/680 of the European Parliament and of the Council, transposed by Law no. 59/2019, of 8 August.

XII. The obtaining of data from communication service providers in criminal proceedings is regulated by other legal provisions: by Articles 187 to 189 and 269(1)(e) of the CPP and by Law no. 109/2009, of 15 September (Cybercrime Law), which transposes into the domestic legal system Framework Decision no. 2005/222/JHA of 24 February on attacks against information systems, and aligns domestic law with the Council of Europe Convention on Cybercrime (Budapest, 2001), ratified by Portugal.

XIII. The Constitutional Court did not declare that the effects of the declaration of unconstitutionality with general binding force, as per judgement no. 268/2022, extend to res judicata, in accordance with Article 282(3) of the Constitution, so this declaration of unconstitutionality does not constitute grounds for the revision of a judgement under article 449(1)(f) of the CPP.

XIV. The declaration of invalidity of Directive no. 2006/24/EC by the Court of Justice of the European Union (CJEU), by judgement of 08.04.2014, in preliminary ruling requests submitted under Article 267 of the TFEU (in the joined cases Digital Rights Ireland Ltd (C-293/12) and Kärntner Landesregierung (C-594/12), pre-dating the judgement under which the appellant was convicted, does not constitute grounds for revision of the judgement referred to in Article 449(1)(g) of the CPP, according to which a revision is admissible when 'a binding judgement of the Portuguese State, issued by an international instance, is incompatible with the conviction or raises serious doubts about its fairness.'

XV. In addition to the law requiring that the judgement rendered by an international instance be subsequent to the conviction, the judgement of the CJEU does not constitute 'a binding judgement' on the Portuguese State, within the meaning of this provision, which was designed for the decisions of the European Court of Human Rights (considering Article 46(1) of the ECHR).

XVI. A judgement of the CJEU that, in a preliminary appeal, declares a directive invalid under Article 267 of TFEU, is addressed directly to the judicial body that referred the matter to the CJEU; the fact that the CJEU's decision constitutes sufficient reason for any other judicial body to consider such an act invalid due to the general obligation to ensure the primacy of Union law, refraining from acts contrary to it that might impair its effectiveness (in this sense, one can speak of an erga omnes effectiveness – see CJEU

judgement C-66/80 of 13 May, 1981), does not confer upon it the status of a party directly affected by that decision, so it should not be considered as a binding judgement serving as a ground for revision.

XVII. Thus, as there are no grounds, the revision of the judgement is denied.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:STJ:2023:191.17.1JELSB.K.S1.EC/

III. COURTS OF APPEAL

LISBON COURT OF APPEAL

- **Judgement of the Lisbon Court of Appeal of 26-01-2023**
  Case no. 50644/21.0YIPRT-A.L1-6
  Rapporteur: Judge Ana Azeredo Coelho

I) The confidentiality of telecommunications is one dimension of the right to privacy and family life and the right to the inviolability of the home and correspondence, with independent recognition in the Constitution.

II) In the field of telecommunications, it is necessary to distinguish basic data (technical support and connection elements unrelated to the communication itself), traffic data (elements related to the communication but not involving its content), and content data (elements related to the actual content of the communication).

III) The elements related to aspects administratively collected during the contracting of the telecommunications service do not pertain to the privacy of the person's life or their intimate sphere in terms of being protected in the context of the legal goods protected by the Constitution.

IV) The Constitution, by prohibiting interference by authorities in telecommunications, safeguarding the established framework regarding criminal judicial proceedings, does not refer to the elements or basic data of a technical or administrative nature that the operating companies may possess due to the established contract.

V) Information such as the address of the contracting consumer is not informative data that benefits from the special access framework established for telecommunications, and the operator is only bound by a duty of confidentiality in this regard.
VI Neither the specific framework applicable to telecommunications operators nor the general regime for the protection of personal data establish the generic protection obligations that are enshrined as duties of professional secrecy.
VII) Telecommunications operators are subject to a duty of confidentiality regarding the address of customers, but this does not constitute a duty of professional secrecy nor does it fall within the scope of the prohibition of interference in telecommunications outside that established in criminal proceedings.
VII) Article 418 of the Code of Civil Procedure does not distinguish between administrative services of public entities and/or private entities.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2023:50644.21.0YIPRT.A.L1.6.BC/

- **Judgement of the Lisbon Court of Appeal of 26-01-2023**
  Case no. 8561/19.4T9LSB.L1-5
  Rapporteur: Judge Ana Cláudia Nogueira

I - The crime of 'Violation of the duty of confidentiality' provided for in Article 51(1) of Law no. 58/2019, of 8 August (previously Article 47(1) of Law no. 67/98, of 26 October) governs the protection of personal data.
II - It is a statutory crime that, in one of its objective elements, refers to another non-criminal law - the one that establishes professional secrecy - resulting from the combination of both a symbiosis of the protection of legal interests related to the right to privacy and the right of each individual not to be used as a source of information for third parties against their will, as well as to control the information that is provided, in the exercise of a true right of informational self-determination.
III - The access by a doctor to the clinical information of a family member, archived in the facilities of the healthcare institution where they work, and the transmission of its contents to a third party without the consent of the person concerned or just cause, while

violating the professional secrecy to which the agent, being a doctor, was subject, directly affects these legal interests.

IV - The existence of a doctor/patient relationship between the agent (doctor) and the holder of the clinical information transmitted/disclosed does not constitute an element of the type of crime, nor does the fact that there was legitimate access by that doctor to that data. Therefore, the accusation is not null and void for violating the provisions of Article 283(3)(b) of the Code of Criminal Procedure, as it does not contain facts from which it can be inferred that the accused provided the assistant with medical care or clinical observation justifying access to their clinical information.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2023:8561.19.4T9LSB.L1.5.08/

- **Judgement of the Lisbon Court of Appeal of 16-03-2023**
  Case no. 73345/21.4YIPRT-A.L1-2
  Rapporteur: Judge Orlando Nascimento

1. The 'principle of the prevalence of the overriding interest' established by Article 135(3) of the CPP determines that, for the purposes of the procedural act of summoning for the purposes of a special action for the fulfilment of pecuniary obligations subsequent to an injunction, the right to privacy of the residence of a user of an electronic communications network should give way to the right of access to justice of the operating company of another electronic communications network.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2023:73345.21.4YIPRT.A.L1.2.69/

- **Judgement of the Lisbon Court of Appeal of 02-05-2023**
  Case no. 12234/21.0T8LSB.L1-7
  Rapporteur: Judge Luís Filipe Sousa

I - The online biography of the applicant published by Wikipedia constitutes the joint processing of personal data for the purposes stipulated in Regulation (EU) 2016/679 (General Data Protection Regulation).

II - Respect for private and family life (Article 7 of the Charter of Fundamental Rights) has the same meaning and scope as the meaning and scope given to Article 8(1) of the ECHR, as interpreted by the case law of the European Court of Human Rights.
III - Freedom of expression and information (Article 11 of the Charter of Fundamental Rights) has the same meaning and scope as the meaning and scope given to Article 10 of the ECHR, as interpreted by the case law of the European Court of Human Rights.
IV - With regard to the requirement that the processing of personal data is necessary for the pursuit of legitimate interests, derogations and restrictions to the principle of the protection of personal data must occur only to the extent strictly necessary.
V - The right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society, balanced with other fundamental rights, in accordance with the principle of proportionality.
VI - Relevant criteria for weighing the right to respect for private life against the right to freedom of expression include: the contribution to a debate of public interest, the degree of notoriety of the person affected, the subject of the report, the previous behaviour of the person in question, the content, form, and consequences of the publication, the manner and circumstances in which the information was obtained, as well as its accuracy.
VII - A distinction must be made between factual statements and value judgements since the materiality of the former can be proven, whereas the latter do not lend themselves to a demonstration of their accuracy.
VIII - With regard to imputations of facts, proof of good faith should be admitted, provided that the person (e.g. journalist) had, at the time of publication, sufficient reason to believe that the information was true, for which reason they should not be penalised.
IX - Given the important role played by the Internet in increasing public access to news and facilitating the dissemination of information, the function of bloggers and social media users can also be assimilated to that of 'public watchdogs' for the purposes of protection under Article 10 of the ECHR.
X - Although, in general, the rights of the person protected by Articles 7 and 8 of the Charter (private and family life and protection of personal data) prevail over the legitimate interest of Internet users potentially interested in accessing the information in question, this balance may, however, depend on the relevant circumstances of each case, in particular the nature of that information and its sensitivity to the private life of the person

concerned, as well as the interest of the public in having access to that information, which may vary, in particular, according to the role played by that person in public life.

XI - When the person concerned plays a role in public life, they must demonstrate an increased degree of tolerance, as they are inevitably and knowingly exposed to public scrutiny.

XII - It is the responsibility of the person who requests the removal of references to prove the manifest inaccuracy of the information contained in said content or, at least, of a part of that information that does not have a minor character in relation to the entirety of that content.

XIII - In order to avoid imposing an excessive burden on this person that could harm the effective exercise of the right to removal of references, it is solely up to them to provide the evidence that, given the circumstances of the specific case, can reasonably be required to demonstrate this manifest inaccuracy.

XIV - The search engine operator cannot be required to investigate the facts and, to that end, to engage in an adversarial debate with the content provider in order to obtain the missing elements regarding the accuracy of the content presented.

XV - The right to be forgotten 'can be defined as a fundamental right of personality protected by the principle of human dignity, according to which the holder, an individual or collective person, has the right to informational self-determination, i.e. they can request the erasure, removal, or blocking of the dissemination of data, whether lawful or not, concerning them, found in various media, that no longer have public, judicial, historical, or statistical interest, or that are not prohibited by law. Therefore, it is not about eliminating all references to past events, but only about avoiding the unnecessary and harmful exposure of events that are devoid of current public interest. In short, it expresses a power of self-control over one's own personal data.'

XVI - The applicant's right to be forgotten is justified in a context where:

- in 1989, they allegedly committed acts that later led to an indictment by the Public Prosecutor's Office for the offence of aggravated theft;
- no trial took place;
- nothing has been proven in the case file to the effect that, if such events had occurred, they would have generated significant social alarm, either at local or national level, i.e. the existence of an uncontroversial original public interest has not been demonstrated;

- if such a crime has occurred, the respective criminal proceedings have been statute-barred, at least since 2008;
- there is no current public interest in ascertaining whether such events occurred in 1989, especially since the online biographies do not indicate the subsequent commission of similar acts by the applicant, nor has it been demonstrated that, at the time of the filing of the procedure, the applicant had any intention of holding new public positions, e.g. consul.

XVII - According to Article 17(1) of Regulation no. 20016/679, the data subject has the right to have their data erased by invoking one of the reasons listed in points (a) to (f), without the need to demonstrate that the processing generates actual or potential harm.

XVIII - In the context of personal data processing, Regulation no. 2016/679 provides for the existence of specialised personal data that are subject to even more restrictive treatment, and the processing of personal data revealing political opinions is prohibited (Article 9(1)).

XIX - As per this legal framework, the Defendant and the Unknown Defendants were not allowed process the applicant's personal data indicating their political opinions, specifically, proximity to leaders of the (...) Party, connection to this party, donation of money to this party, participation in a rally, as well as support for ZM.

XX - For the purpose of assessing the requirement of the common precautionary procedure consisting of periculum in mora, personality rights are naturally subject to damage that is difficult to repair, since the infringement of these rights can only be economically compensated, never fully repairing the damage due to the non-pecuniary nature of the assets subject to these rights.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2023:12234.21.0T8LSB.L1.7.AB/

- **Judgement of the Lisbon Court of Appeal of 02-05-2023**
  Case no. 998/19.5T8LSB.L1-6
  Rapporteur: Judge Jorge Almeida Esteves

I - Telecommunications companies are subject to confidentiality duties, according to Article 48 of Law no. 5/2004, of 10.02, the Electronic Communications Law (in force at

the time of the relevant facts), and Article 4(1) of Law no. 41/2004, of 18.08, the Law on the Protection of Personal Data and Privacy in Telecommunications, preventing them from disclosing or allowing third parties to access such data.
II - Since the cause of action is based on the disclosure by the 1st defendant, an employee of the 2nd defendant, which is a telecommunications company, of all the content that the plaintiff had on her mobile phone (list of calls made, telephone contacts, messages, traffic data, data relating to the destination, route, time, and duration of telephone calls made to and from the aforementioned plaintiff's mobile phone number, and records of messages on the mobile phone and in the diary) and since it has not been proven that the 1st defendant accessed this data, only accessing, on a specific day, the communications made by the plaintiff, and not even proving their disclosure, the compensation claim fails for lack of evidence of an unlawful act susceptible to causing harm for the purposes of tort liability.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2023:998.19.5T8LSB.L1.6.B2/

- **Judgement of the Lisbon Court of Appeal of 13-07-2023**
  Case no. 12234/21.0T8LSB.L1-7
  Rapporteur: Judge Luís Filipe Sousa

I - The online biography of the applicant published by Wikipedia constitutes the processing of their personal data.
II - However, Regulation (EU) 2016/679 (General Data Protection Regulation) does not apply to this case as none of the alternative requirements set out in Article 3 of the Regulation (territorial scope) are met.
III - In the context of an interlocutory procedure in which the decision to be taken therein can no longer be the subject of an appeal, the initiation of a preliminary ruling is not mandatory, provided that each party is able to bring or require the filing of a main action, during which the issue - provisionally resolved in the summary proceedings - can be reconsidered as to its substantive merits and be the subject of a preliminary ruling (Judgements of the Court of Justice of 24.5.1977, Hoffman – La Roche, 107/76, and of 27.10.1982, Case Morson, C-35/82).

IV - Respect for private and family life (Article 7 of the Charter of Fundamental Rights of the European Union - CFREU) has the same meaning and scope as the meaning and scope given to Article 8(1) of the European Convention on Human Rights - ECHR, as interpreted by the case law of the European Court of Human Rights - ECtHR.

V - Freedom of expression and information (Article 11 of the CFREU) has the same meaning and scope as the meaning and scope given to Article 10 of the ECHR, as interpreted by the case law of the ECtHR.

IX - Given the important role played by the Internet in increasing public access to news and facilitating the dissemination of information, the function of bloggers and social media users can also be assimilated to that of 'public watchdogs' for the purposes of protection under Article 10 of the ECHR.

XI - When the person concerned plays a role in public life, they must demonstrate an increased degree of tolerance, as they are inevitably and knowingly exposed to public scrutiny.

XIII - In order to avoid imposing an excessive burden on this person that could harm the effective exercise of the right to removal of references, it is solely up to them to provide the evidence that, given the circumstances of the specific case, can reasonably be required to demonstrate this manifest inaccuracy.

XV - The applicant's right to be forgotten is justified in a context where:

a.- in 1989, they allegedly committed acts that later led to an indictment by the Public Prosecutor's Office for the offence of aggravated theft;

b.- no trial took place;

c.- nothing has been proven in the case file to the effect that, if such events had occurred, they would have generated significant social alarm, either at local or national level, i.e. the existence of an uncontroversial original public interest has not been demonstrated;

d.- if such a crime has occurred, the respective criminal proceedings have been statute-barred, at least since 2008;

e.- there is no current public interest in ascertaining whether such events occurred in 1989, especially since the online biographies do not indicate the subsequent commission of similar acts by the applicant, nor has it been demonstrated that, at the time of the filing of the procedure, the applicant had any intention of holding new public positions, e.g. consul.

XVI - By expressing a desire to have a political intervention, the applicant naturally raises the interest of the public/Internet users, and it is certain that any political intervention gives rise to a debate of public interest on the suitability and merit of the political ideals they espouse (explicitly or implicitly).

XVII - Public intervention in political events, regardless of its extent, is by nature an act within the public sphere, the purpose of political activity being the transformation of society and, for this very reason, any such activity is subject to public scrutiny.

XVIII - Anonymous manifestations are admissible as part of the right to freedom of expression, considering that the protection of anonymity stems from the principle of informational self-determination. However, this right - as in any situation of conflict or collision - gives way to other rights or other constitutionally protected interests, especially in case of unlawfulness.

XIX - Wikipedia is not an intermediary service provider for the purposes of exemption from a general obligation to monitor the information it disseminates (see Articles 12 to 15 of Directive 2000/31/EC and Articles 4(5) and 12 of Decree-Law no. 7/2004, of 7 January).

XX - For the purpose of assessing the requirement of the common precautionary procedure consisting of periculum in mora, personality rights are naturally subject to damage that is difficult to repair, since the infringement of these rights can only be economically compensated, never fully repairing the damage due to the non-pecuniary nature of the assets subject to these rights.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2023:12234.21.0T8LSB.L1.7.91/

- **Judgement of the Lisbon Court of Appeal of 11-10-2023**
  Case no. 1232/19.3PBFUN.L1-3
  Rapporteur: Judge Cristina Almeida de Sousa

Text messages received on a mobile phone are not metadata, just as interceptions of telephone conversations are not metadata. Intercepting phone conversations, being inherently a covert means of obtaining evidence, as its success depends exclusively and directly on the unawareness of the parties involved that their phone communications are

being intercepted, directly affect the content of communications in real-time and for the future.

The legal framework set out in Articles 187 to 189 of the CPP, which governs the substantive prerequisites for the admissibility of telephone interceptions, has not been affected in the slightest by the declaration of unconstitutionality decided, with general binding force, by judgement of the TC no. 268/2022.

Although the reference contained in Article 21(2) of Law no. 112/2009, to Article 82-A of the CPP, does not remove from the scope of this reference the submission of the decision to prior adversarial proceedings, in this very special case, the adversarial principle is deemed fulfilled in the defence directed against the accusation itself. Given the mandatory nature of the ex-officio determination of the pecuniary amount intended to compensate for the damages resulting from the crime of domestic violence suffered by the victim, there is no element of surprise for the defendant arising from this decision. The accused has the opportunity to contest it either in response to the accusation or during the preliminary hearing, using the procedural rights inherent in the legal status of defendant.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2023:1232.19.3PBFUN.L1.3.48/

- **Judgement of the Lisbon Court of Appeal of 09-11-2023**
  Case no. 4961/20.5T8LRS-A.L1-2
  Rapporteur: Judge Carlos Castelo Branco

I) The name and address of an individual constitute personal data that may be disclosed for the pursuit of legitimate interests of the data controller or a third party to whom the data is communicated, provided that the interests or the rights, freedoms, and guarantees of the data subject do not prevail.

II) Professional secrecy, in general, is established based on various interests, namely that of the institutions themselves, in whose activity the principle of trust of the individuals, the direct 'clients' of the entities that provide services or carry out an activity, is particularly relevant, and the safeguarding of privacy is at stake, as well as that of third parties - indirect 'clients' who relate to these institutions the former.

III) In the context of private legal relationships, the breach of professional secrecy takes on exceptional characteristics and should be assessed in a logic of indispensability, limiting itself to the minimum essential for achieving the intended values.
IV) The conflict between the duty to cooperate with the administration of justice and the duty of professional secrecy must be resolved on a case-by-case basis based on the principle of proportionality.
V) The exceptional measure of breaking professional secrecy is justified when the information sought, covered by professional secrecy, is crucial for the realisation of the judicially determined purpose, and the only foreseeable means of fulfilling a right of the applicant, judicially recognised and in execution for a long time.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2023:4961.20.5T8LRS.A.L1.2.75/

- **Judgement of the Lisbon Court of Appeal of 22-11-2023**
  Case no. 271/19.9T8FNC-A.L1-4
  Rapporteur: Judge Paula Pott

Liquidation for the enforcement of a labour court judgement - Article 390(2) of the Labour Code - Appeal of the ruling that did not admit means of proof - Failure to indicate the documents that must accompany the appeal separately - Electronic submission of the appeal - Need for evidence - Purpose of the liquidation - Exclusivity clause.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2023:271.19.9T8FNC.A.L1.4.C9/

PORTO COURT OF APPEAL

- **Judgement of the Porto Court of Appeal of 07-12-2022** (published in 2023)
  Case no. 5011/22.2JAPRT-A.P1
  Rapporteur: Judge Pedro Vaz Pato

I - Having the judgement of the Constitutional Court declared the unconstitutionality, with binding force, of Articles 4, 6, and 9 of Law no. 32/2008, of 17 July (Law on the retention of data generated or processed in the context of the provision of electronic communications services), we cannot try to circumvent that judgement by 'letting in through the window' what it 'closed the door' to; in other words, we cannot resort to other rules to achieve the same effect as the application of the rules declared unconstitutional without those other rules containing those guarantees that are lacking in these rules and that led to that declaration of unconstitutionality.
II - It is therefore not legally possible to resort, for this purpose, to the frameworks of Articles 187 and 189 of the Code of Criminal Procedure (relating to real-time communications, not to the retention of data from past communications), Law no. 417-2008, of 18 August (related to contractual protection in the context of relations between companies providing electronic communications services and their customers, a field distinct from that of criminal investigation), and Law no. 109/2009, of 15 September (Cybercrime Law).
III - Courts cannot substitute for the legislator by filling in omissions that result in serious inconveniences for criminal investigations.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2022:5011.22.2JAPRT.A.P1.85/

- **Judgement of the Porto Court of Appeal of 18-01-2023**
  Case no. 344/20.5IDPRT-B.P1
  Rapporteur: Judge José António Rodrigues da Cunha

I - With the entry into force of Law no. 32/2008, of 17.07, the criminal procedural framework provided for in Articles 187 to 189 of the CPP was repealed in what regards retained data.
II - The framework of Articles 187 to 189 of the CPP is not applicable to the data covered by Law no. 32/2008, and this is not prevented by the declaration of unconstitutionality, with general binding force, of the provisions of Articles 4, 6, and 9 of that Law.
III - Even if it were otherwise, allowing access to traffic data and location data based on those provisions would clearly violate European law and the interpretation thereof by the

CJEU, constituting a more intense and disproportionate infringement of fundamental rights to privacy and the protection of personal data provided for in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU) than Directive no. 2006/24/EC, which has since been declared invalid.

IV - Indeed, the framework of Articles 187 and 189 of the CPP does not even comply with the requirements of the Directive, contrary to what happened with Law no. 32/2008, which, in fact, went beyond what was required with regard to rules ensuring the security of retained data and criteria governing access to stored data.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2023:344.20.5IDPRT.B.P1.99/

- **Judgement of the Porto Court of Appeal of 18-01-2023**
  Case no. 47/22.6PEPRT-P.P1
  Rapporteur: Judge João Pedro Pereira Cardoso

I - The grounds for unconstitutionality declared, with general binding force, in judgement of the TC no. 268/2022, of 19.04, do not apply to the interception of traffic data, including mobile phone location, in real time during an investigation.

II - The interception of traffic data, such as detailed billing, including calls made and received (trace-back), mobile phone locations, and the identification of numbers that contact them and roaming communications, when obtained in real time during the investigation concerning suspects or defendants (Article 187(4)(a) of the CPP), does not imply a disproportionate interference in the fundamental rights to respect for private and family life and the protection of personal data provided for in Articles 7 and 8 of the CDFUE, as well as in Article 35(1) and (4) and Article 26(1) of the CRP.

III - As with content data (wiretapping), the interception of traffic data, including cell locations, in real time, during the investigation, presupposes the interception or monitoring of this data, as with wiretapping, and not the use of a database kept or stored by operators concerning all subscribers and registered users, which is the only situation referred to in judgement of the TC 268/2022 and Law no. 32/2008, of 17 July.

IV - Allowing access to and valuation in criminal proceedings of metadata obtained and processed for billing purposes between the customer and the operator is the same as

consenting to their use for a purpose other than that for which they were stored, defrauding the scope of regulation provided for in Law 41/2004, of 18 August, to assist criminal investigations.

V - With regard to traffic data, including cell locations, in real time, the extension framework contained in Article 189(2) continues to apply to the catalogue crimes provided for in Article 187(1), both of the Code of Criminal Procedure. In that case, the special framework of Article 18(1) and (3) of Law no. 109/2009, of 05.09 (Cybercrime Law) also continues to apply to the catalogue crimes provided for in that law.

VI - The accused or suspect, whose traffic data and location data are to be intercepted, benefits from the control guarantees established for wiretapping in Articles 187 and 188 of the CPP, which apply here mutatis mutandi, and there is no reason to impose on the interception of traffic data, in real time, a communication that is dispensed with in the interception of content data (wiretapping), under the pretext of the right to informational self-determination and effective judicial protection provided for in Article 35(1) and Article 20(1) of the CRP.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2023:2748.22.0JAPRT.A.P1.72/

- **Judgement of the Porto Court of Appeal of 01-02-2023**
  Case no. 1443/21.1T8AMT-B.P1
  Rapporteur: Judge João Pedro Pereira Cardoso

I - The grounds for unconstitutionality declared, with general binding force, in judgement of the TC no. 268/2022, of 19.04, do not apply to the interception of traffic data, including mobile phone location, in real time during an investigation.

II - The interception of traffic data, such as detailed billing, including calls made and received (trace-back), mobile phone locations, and the identification of numbers that contact them and roaming communications, when obtained in real time during the investigation concerning suspects or defendants (Article 187(4)(a) of the CPP), does not imply a disproportionate interference in the fundamental rights to respect for private and family life and the protection of personal data provided for in Articles 7 and 8 of the CDFUE, as well as in Article 35(1) and (4) and Article 26(1) of the CRP.

III - As with content data (wiretapping), the interception of traffic data, including cell locations, in real time, during the investigation, presupposes the interception or monitoring of this data, as with wiretapping, and not the use of a database kept or stored by operators concerning all subscribers and registered users, which is the only situation referred to in judgement of the TC 268/2022 and Law no. 32/2008, of 17 July.
IV - Allowing access to and valuation in criminal proceedings of metadata obtained and processed for billing purposes between the customer and the operator is the same as consenting to their use for a purpose other than that for which they were stored, defrauding the scope of regulation provided for in Law 41/2004, of 18 August, to assist criminal investigations.
V - With regard to traffic data, including cell locations, in real time, the extension framework contained in Article 189(2) continues to apply to the catalogue crimes provided for in Article 187(1), both of the Code of Criminal Procedure. In that case, the special framework of Article 18(1) and (3) of Law no. 109/2009, of 05.09 (Cybercrime Law) also continues to apply to the catalogue crimes provided for in that law.
VI - The accused or suspect, whose traffic data and location data are to be intercepted, benefits from the control guarantees established for wiretapping in Articles 187 and 188 of the CPP, which apply here mutatis mutandi, and there is no reason to impose on the interception of traffic data, in real time, a communication that is dispensed with in the interception of content data (wiretapping), under the pretext of the right to informational self-determination and effective judicial protection provided for in Article 35(1) and Article 20(1) of the CRP.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2023:47.22.6PEPRT.P.P1.AB/

- **Judgement of the Porto Court of Appeal of 28-02-2023**
  Case no. 1443/21.1T8AMT-B.P1
  Rapporteur: Judge João Ramos Lopes

I - Since the claim formulated in these proceedings is for the annulment of the electoral process that had been taking place (with the consequent opening of a new electoral process), the fact that the election has taken place does not result in the disappearance of

the object of the proceedings and/or, much less, that the outcome sought by the applicants would have been achieved outside the scope of the requested remedy.
II - The lesser expeditiousness given to its processing does not determine the supervening uselessness (and impossibility) of the precautionary procedure - since the subject matter of the dispute has not ceased (because the interest of the applicants has not been satisfied by other means and/or has not become impossible to achieve), there is no extinction of the proceedings due to the supervening uselessness (or impossibility) of the dispute.
III - In the context of a procedure seeking the annulment of an ongoing electoral process and the initiation of a new electoral process, the legitimacy of refusing cooperation (Article 417(3)(c) of the CPC) based on the duty of confidentiality (and/or protection of personal data) invoked by the defendant, an institution with the functions of Bank 1... in favour of its members and also the performance of other acts of banking activity, in order to avoid joining a list of its members in full enjoyment of their rights, is to be rejected.
IV - As members (or cooperators), the applicants have the right to participate in the electoral process aimed at electing the governing bodies of the defendant - and having the right to participate in such an act of the defendant's internal life, they have the right to know the relevant elements of interest in such an electoral act (not only to participate in such an act as candidates but also to oversee the entire process), and are therefore individuals entitled to share knowledge (share the secret) and to have access to the 'electoral rolls' (to know the identity of the other members).
V - The situation referred to in the previous points does not involve any processing, circulation, or sharing of data on natural persons, as defined in Articles 2(1) and 4(2) of the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data).
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2023:1443.21.1T8AMT.B.P1.C7/

- **Judgement of the Porto Court of Appeal of 09-03-2023**
  Case no. 8228/18.0T8PRT-C.P1
  Rapporteur: Judge Carlos Portela

I - The rules on the inadmissibility of processing/communication of personal data provided in the LPDP are not absolute and allow for exceptions to enable the processing of such personal data when this is necessary for the declaration, exercise, or defence of a right, whether it be in a judicial process, administrative process, or extrajudicial process.
II - The notification to the debtor, referred to in Article 583(1) of the Civil Code, that their creditor has assigned the claim to another party, can be made through the summons for enforcement proposed by the assignee creditor against the enforced opponents.
III - In the opposition of the executed, the substantive rules governing the distribution of the burden of proof, as provided for in Article 342 of the Civil Code, remain unchanged. It is the responsibility of the executed party who raises objections to prove the facts that prevent, modify, or extinguish the right of the executing party, while the executing party is responsible for proving the facts establishing the executing right.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2023:8228.18.0T8PRT.C.P1.A8/

- **Judgement of the Porto Court of Appeal of 29-03-2023**
  Case no. 47/22.6PEPRT-Z.P1
  Rapporteur: Judge Maria Joana Grácio

The declaration of unconstitutionality with general binding force of Article 4, in conjunction with Articles 6 and 9, all of Law no. 32/2008, of 17 July, does not prevent the possibility of authorising the obtaining of traffic or cell location data retained under Law no. 41/2008, of 18 August, based on Article 189(2) of the Code of Criminal Procedure.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2023:47.22.6PEPRT.Z.P1.16/

- **Judgement of the Porto Court of Appeal of 24-05-2023**
  Case no. 398/23.2KRPRT-A.P1
  Rapporteur: Judge Eduarda Lobo

I - The declaration of unconstitutionality in Constitutional Court Judgement no. 268/2022 applies only to data - traffic and location data - previously retained/stored, to the generalised and undifferentiated retention of traffic data, and not to real-time traffic data; therefore, the declaration of unconstitutionality does not affect traffic data generated at the same time as content data (interception of telephone conversations or telephone communications), since both are obtained in real time.

II - Obtaining and transmitting traffic and location data in real time, including the record of calls made and received, detailed billing, and the respective cell location, related to intercepted communications, does not imply a disproportionate interference with the fundamental rights to respect for private and family life and the protection of personal data provided for in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU); this is because, like content data (wiretapping, the interception of traffic data in real time would not cover, in a generalised manner, all subscribers and registered users, but only the suspects or defendants under investigation, and would therefore not be covered by the declaration of unconstitutionality of Constitutional Court Judgement no. 268/2022.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2023:398.23.2KRPRT.A.P1.18/

- **Judgement of the Porto Court of Appeal of 08-05-2023**
  Case no. 7251/22.5T8PRT.P1
  Rapporteur: Judge Fernanda Almeida

I - The right to one's image encompasses, firstly, the right to define one's own self-exposure, i.e. the right of each individual not to be photographed and not to have their portrait displayed in public without their consent; secondly, it includes the right not to have one's image presented in a graphically offensive or malevolently distorted or unfaithful manner ('falsification of personality').

II - Article 79 of the CC establishes the right to self-determination of one's external image, following the general protection of personality enshrined in Article 70, granting individuals the choice of how they present themselves to others, including the when and

the how (clothing, accessories, etc.), and the right to define the terms and conditions under which their portrait can be taken and used by third parties.

III - When an individual chooses to make certain behaviours or images public, especially on social media, that are protected by the right to privacy, they are not waiving their right to personality (which includes the right to image) but are autonomously exercising it, thereby sovereignly defining their self-exposure.

IV - The right to informational self-determination is a new legal application of the right to privacy and does not cease to exist simply because an individual does not exercise it or make efforts to defend it.

V - Freedom of expression includes the publication of photographs, and this is an area where the protection of the reputation and rights of third parties is of particular importance, as photographs may contain personal, even intimate, information about an individual or their family.

VI - If a media outlet aims to inform readers of a magazine published nationwide that a certain young woman, the daughter of a party leader, is also entering the political scene - which can be considered a matter of public and national interest and therefore legitimate - it does not seem appropriate to the news and proportionate to that purpose to use photographs of her published without her consent, altering them and showing her in more daring poses or in private life situations.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2023:7251.22.5T8PRT.P1.87/

- **Judgement of the Porto Court of Appeal of 23-10-2023**
  Case no. 728/22.4T8OVR-A.P1
  Rapporteur: Judge Ana Paula Amorim

I - The insurer (including directors, employees, agents, and other assistants of the insurer) is bound by professional secrecy in relation to information learnt in the context of entering into a contract, including the client's address, and any refusal to provide this information to the court is legitimate.

II - Aiming solely at promoting the constitution and notification of the defendant as the faithful custodian of the seized assets, as well as initiating seizure proceedings at their

residence, in contrast to the principle safeguarding the privacy of private life, the public interest in the administration and dispensation of justice should prevail. Therefore, confidentiality can be waived for that specific purpose.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2023:728.22.4T8OVR.A.P1.6C/

COIMBRA COURT OF APPEAL

- **Judgement of the Coimbra Court of Appeal of 26-04-2023**
  Case no. 840/22.0T9LRA-A.C1
  Rapporteur: Judge Ana Carolina Cardoso

I - The computer search referred to in Article 15(1) of the Cybercrime Law consists of a preliminary search of the suspected electronic device to determine whether there are any data stored on it that are relevant to the evidence; if that is the case, the device is seized for the purpose of extracting the data.
II - The existence of specific and determined computer data stored in a computer system, obtained through a preliminary computer search, is different from the extraction of relevant data from the computer equipment where they were found, as well as their inclusion in the case file, which is why that search should never be confused with the 'inclusion' of the material in the case file.
III - The time limit referred to in Article 15(2) of the Cybercrime Law relates to that preliminary search, not to the extraction of relevant data from the computer equipment for the purposes of their inclusion in the case file, which is provided for in Article 16 of the same law.
IV - When computer data or documents are seized, the content of which may reveal personal or intimate information that could compromise the privacy of the respective holder or a third party, they must be submitted to the judge before being included in the case file, under penalty of nullity, for the issuance of the order referred to in Article 16(3) of the Cybercrime Law.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRC:2023:840.22.0T9LRA.A.C1.7A/

- **Judgement of the Coimbra Court of Appeal of 27-09-2023**
  Case no. 13/20.6PEVIS.C1
  Rapporteur: Judge Maria Teresa Coimbra

I - Basic data refers to access to the network and allows for the identification of the user of the equipment (IP protocol addresses, civil identity of the holder, telephone numbers, and e-mail addresses), and traffic data reveals circumstances of communications, such as the location of the parties involved in the communication, duration, date, time of interpersonal communications, but also those that do not involve interpersonal communication.
II - In judgement no. 268/2022, of 19 April, the Constitutional Court declared, with general binding force, that it violates the constitutional principle of proportionality in restricting the rights to privacy, confidentiality of communications, free development of personality, informational self-determination, and effective judicial protection in the collection, recording, conservation, and access to personal data, traffic, and location concerning all subscribers and registered users in electronic communications service providers, in a generalised and undifferentiated manner and in relation to all means of electronic communication, for one year, and for criminal purposes, in accordance with Articles 4, 6, and 9 of Law no. 32/2008, of 17 July.
III - The absence of notification to the concerned party that their data had been accessed was also criticised, based on the understanding that the right to informational self-determination and effective judicial protection would be disproportionately compromised.
IV - The Constitutional Court considers that the retention of basic data, as a restrictive measure of the rights to privacy and informational self-determination, respects the principle of proportionality, since it only identifies the users of the means of communication and does not involve the analysis of any communication.
V - In judgement no. 268/2022, of 19 April, the Constitutional Court did not scrutinise or criticise any provisions other than those of Articles 4, 6, and 9 of Law no. 32/2008, of 17

July, or any other legal diplomas, and therefore the declaration of unconstitutionality it issued does not have the potential to cover any and all evidence obtained by digital means.
VI - The Constitutional Court did not consider that the provisions of the CPP that allow obtaining and including in the case file data on cell location or records of conversations or communications related to crimes provided for in Article 187(1) were unconstitutional, nor did it rule out the possibility of retaining data under other legislation, for example, for contractual purposes, such as Law no. 41/2004, of 18 August, which provides for the retention of traffic data for a period of 6 months.
VII - Evidence obtained from data stored by telecommunications operators is valid within the limits legally imposed by the laws that remain in force and which continue to provide for the possibility of obtaining, storing, and transmitting such data.
VIII - Information from Ascendi, indicating the time and location of passage of certain vehicles on national highways, information from Via Verde, indicating the existence or absence of records regarding certain vehicles, and from Brisa, reporting a transfer of contractual position in a concession contract granted by the State and the non-processing of requested data, bank information, additions to reports drawn up following direct observation by law enforcement officers, do not conflict with the declaration of unconstitutionality in question because they are not functional data necessary for the establishment of communication, nor are they covered by the considerations that underpinned the judgement of unconstitutionality.
IX - Prohibited evidence does not necessarily mean prohibited valuation. If prohibited evidence has been used and it has been the only evidence on which the conviction was based, the decision must be overturned and the accused acquitted; if the prohibited evidence has been excluded from the reasoning of the decision, the decision must be upheld, unless there are other reasons; if the prohibited evidence has coexisted with other admissible evidence, it must be determined what contribution the remaining and legitimate evidence made to the conviction.
X - The determination of the specific sentence is the operation that summarises the trial, reflecting the intended purpose of the sentence, and it is aimed at both the defendant and society, due to the role that the courts must play in fostering social peace.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRC:2023:13.20.6PEVIS.C1.F0/

ÉVORA COURT OF APPEAL

- **Judgement of the Évora Court of Appeal of 12-01-2023**

  Case no. 1137/22.0T8PTM-C.E1

  Rapporteur: Judge Anabela Luna de Carvalho

- Both tax confidentiality and banking confidentiality aim to ensure the protection of privacy, a constitutional value (Articles 26 and 35(4) of the CRP), and the public interest of trust in institutions.
- Banking secrecy and tax secrecy are also protected by the General Data Protection Regulation (Article 5(1)(f) 'integrity and confidentiality') and its implementing law, Law no. 58/2019, of 08/08 (Article 20 'duty of secrecy'), since the elements protected by secrecy are contained in totally or partially automated means (Article 2 of the GDPR).
- Article 135 of the CPP establishes the procedural framework for breaking confidentiality, invoking the principle of the prevalence of the overriding interest.
- Article 6 of the GDPR, by listing a series of situations that, in addition to consent, confer lawfulness to the processing, calls for a proportional assessment of the legitimate interests pursued by a third party.
- Since the assets of the couple, consisting of the Applicant and the Respondent, are being listed, the Applicant's particular interest in knowing the real value of these assets (which also belong to her) appears to be more preponderant and relevant, in order to preserve them for the subsequent division that may result from the possible divorce decree, compared to the interest of the Respondent in maintaining the confidentiality of his personal (banking and tax) data containing such information.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRE:2023:1137.22.0T8PTM.C.E1.F5/

- **Judgement of the Évora Court of Appeal of 14-09-2023**

  Case no. 168/23.8T8OLH.E1

  Rapporteur: Judge Tomé de Carvalho

1 - Whenever someone shows a well-founded fear of serious and difficult-to-repair damage to their right, they may request the conservatory or anticipatory measure specifically suitable to ensure the effectiveness of the threatened right.
2 - The measure shall be decreed as long as there is a serious likelihood of the existence of the right and the fear of its harm is sufficiently grounded.
3 - The case law of the Court of Justice asserts that the right to the protection of personal data is not an absolute right and that it must be weighed in order to find a balance with other fundamental rights, in accordance with the principle of proportionality.
4 - In this domain, four criteria are usually found to balance divergent interests and rights: (i) the context and content of the comments, (ii) the responsibility of the authors of the comments, (iii) the measures taken by the applicants and the conduct of the injured party, and (iv) the consequences for the injured parties and the applicants.
5 - Freedom of expression is not an absolute right and has inherent limits and, in the event of a collision or conflict with other rights, it can be restricted or shaped with the intention of valuing the rights to moral integrity, good name and reputation, and to the privacy of private and family life.
6 - Depending on the severity and context of the accusation, outside the dimension of freedom of the press and in the context of public figures, the right to opinion or information gives way - or may give way - to personal goods such as honour and privacy, in the name of the principle of practical concordance, which is an inherent consequence of the principle of proportionality, requiring the coordination and combination of conflicting legal goods in order to avoid the (total) sacrifice of some in relation to others.
7 - However, merely making this statement is not enough, as, in this case, it is necessary not only to dismiss the doctrine of reinforced protection of freedom of expression but also to meet the specific prerequisites that allow the precautionary measure to be considered valid.
8 - The applicant subscribed to a specific service that allows the issuance of positive or negative evaluations regarding their professional performance, and although this subscription does not deprive them of their rights to personal honour and professional consideration, it does open up a space for legitimate, non-abusive criticism and tolerable freedom of expression and information for any client or consumer.

9 - The integration of the concept of difficult-to-repair damage should consider the severity of the foreseeable injury, which must be assessed in light of the impact it will have on the legal sphere of the party involved, calibrated according to the established facts.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRE:2023:168.23.8T8OLH.E1.D9/

- **Judgement of the Évora Court of Appeal of 26-09-2023**
  Case no. 1044/18.1T9EVR.E1
  Rapporteur: Judge João Carrola

1. The subjective type of offence - the aggravated crime of violating rules regarding files and prints, provided for and punishable by Article 43(1) of Law no. 37/2015, on the date of the facts by reference to Article 43(1)(c) and (2) of Law no. 67/98 (currently by reference to Article 46(1) and (2) of Law no. 58/2019) - configures it as a fundamentally intentional crime: it requires knowledge and intent on the part of the agent regarding the deviation or use of personal data in a manner incompatible with the purpose of collection.
2. This legal type of offence also reveals a specific intent that should guide the agent's actions, which is an additional element to the mentioned generic intent.
3. The function of the criminal requirement for knowledge of the fact, in terms of the subjective element, is related to the need for the agent to be aware of everything necessary for a correct orientation of the ethical consciousness towards the legal devaluation specifically linked to the intended action, to its illegal nature.
4. When the agent is unaware of the legal prohibition due to a lack of information or clarification, they should be punished for negligence if, being able and obligated to do so, they neglected to gather the necessary information. If knowledge of the legal prohibition is reasonably indispensable for the agent to be aware of the unlawfulness of the act, error about legal prohibitions excludes intent.
5. Article 16(1) of the Penal Code applies to norms with a slight axiological relevance of conduct. Therefore, when the agent is unaware of the legal prohibition due to a lack of information or clarification, they should be punished for negligence if, being able and obligated to do so, they neglected to gather the necessary information. If knowledge of

the legal prohibition is reasonably indispensable for the agent to be aware of the unlawfulness of the act, error about legal prohibitions excludes intent.

6. The framework extends to errors about the existence of a justification situation, as set out in Article 16(2) of the Penal Code. The intent of the type only includes the representation of the criminal act and the factual assumptions of justifying circumstances.

7. Article 17 of the Penal Code, regarding error about unlawfulness, states that the deficient ethical awareness of the agent does not allow grasping legal and penal values and orienting oneself compliance with the law, except if this deficiency arises from an indifferent personality or an attitude contrary to values, so the culpability of the agent, in addition to being intentional, is reprehensible.

8. This framework focuses on the reprehensibility of the lack of awareness of unlawfulness limited to crimes prohibited in themselves, the so-called natural crimes, where the axiological burden of typification is its characteristic. These are natural crimes, against legal interests that are eminently personal, crimes in themselves (mala in se), such as most of the offences provided for in the Penal Code

9. In the cases referred to in Article 16(1), ignorance of the prohibition is not a problem of [lack of] ethical awareness on the part of the agent [as is the case with errors about prohibition referred to in Article 17 of the Penal Code], but rather a problem of knowledge, which will exclude intent. That is, contrary to what happens with awareness of unlawfulness (Article 17 of the Penal Code), which is presumed in the face of intent, our Penal Code treats prohibitions whose knowledge is reasonably necessary for the agent to be aware of the lawfulness of the act (Article 16(1), Part 2 of the Penal Code) as if they were elements of fact or law of the type of crime, since their knowledge, which is not presumed, is essential for imputing the typical objective act to the agent, with intent.

10. Whenever the lack of knowledge necessary for a correct orientation of the agent's ethical conscience towards the unlawfulness of the act, there is an error that will exclude intent at the level of the type; on the other hand, there is an error that establishes the intent of guilt whenever, having knowledge reasonably indispensable for that orientation, they act in a state of error about the unlawful nature of the act, revealing a lack of harmony with the legal order of values.

11. The defendant, by using the criminal record certificate of a third party without their authorisation, acted knowingly that such a document represents a negative expression of

the privacy of that person's privacy (their criminal record) and against whom it was used. In this context, the defendant was aware of the nature of the data, its restricted use, and that it breached regulatory standards. The defendant's ethical consciousness does not suffer from any vice or deficiency that would prevent them from recognising the unlawfulness of the conduct and the fact, under Article 17 of the Penal Code. Therefore, any error of ignorance and/or lack of knowledge of the unlawfulness of the conduct that would exculpate them cannot be accepted. In other words, the defendant had knowledge and the will to violate the norm and all its factual prerequisites and, in this case, both intentional and negligent conduct are present.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRE:2023:1044.18.1T9EVR.E1.B4/

GUIMARÃES COURT OF APPEAL

- **Judgement of the Guimarães Court of Appeal of 30-03-2023**
  Case no. 11/20.0T8BGC.G1
  Rapporteur: Judge Vera Sottomayor

I - A judgement cannot be deemed null and void for failure to rule does not occur when the exception (issue) has not been sufficiently addressed, nor has it been it formulated in the terms provided for in Article 572(c) of the CPC, has any request been formulated that would require it to be examined.
II - There is an abuse of right when the right, in principle legitimate and reasonable, is exercised in a matter that constitutes a flagrant offence to the prevailing legal sentiment in a particular case.
III - The disciplinary procedure is not null and void, because the evidence produced in it is not null and void either, since there is no violation of banking secrecy as provided for in Article 78 of Decree-Law no. 298/92, of 31 December, when an employer, in this case, a banking institution, uses information, including documents, related to the relationships established between the banking institution and its clients as means of evidence in a

disciplinary process against one of its employees, because everything occurs within the internal scope of the institution itself.

IV - Bank employees are required to adopt an attitude of transparency and to carry out their duties with integrity, suitability, loyalty, and good faith, respecting the legal provisions and the rules issued by the Bank's Management.

V - The disobedience and failure to fulfil the duty of diligence demonstrated by the Plaintiff's conduct, as well as their disloyalty in impersonating their mother, even though their conduct did not cause any harm to the Respondent, is qualified as very serious due to the role of a bank manager that required a different way of acting in the pursuit of interests entrusted to them by their employer.

The plaintiff's conduct irreparably undermined the trust underlying the employment relationship, especially the trust placed in them by the Respondent, both by disregarding the rules and procedures they were obliged to follow and by showing a lack of concern for the consequences of such non-compliance on their subordinates and the duty to impose the same discipline on them.

VI - The dismissal sanction is proportionally appropriate to the case, considering the actions of a bank manager, their culpability revealing a lack of concern for the employer and the fulfilment of their professional duties, and the extent of the employer's interests harmed by the plaintiff's conduct. It is not apparent that any other sanction could be applied, and the fact that the plaintiff has seniority and no prior disciplinary record, on its own, does not preclude the adequacy of the sanction.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRG:2023:11.20.0T8BGC.G1.E9/

- **Judgement of the Guimarães Court of Appeal of 03-10-2023**
  Case no. 241/20.4JAVRL.G1
  Rapporteur: Judge António Teixeira

I - In judgement no. 268/2022, of 19 April, the Constitutional Court did not scrutinise or criticise provisions other than those contained in Articles 4, 6, and 9 of Law no. 32/2008, of 17 July, nor other legal diplomas, namely Articles 187 to 189 of the CPP.

II - Therefore, it is admissible, under the framework outlined in the aforementioned Articles 187 to 189 of the CPP, the interception of communications and the collection of metadata related to it and derived from it, authorised by the investigating judge during an ongoing inquiry.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRG:2023:241.20.4JAVRL.G1.67/

- **Judgement of the Guimarães Court of Appeal of 02-05-2023**
  Case no. 12/23.6 PBGMR-A.G1
  Rapporteur: Judge Armando Azevedo

I - Law no. 32/2008, of 17 July, which transposed into the domestic legal system Directive no. 2006/24/EC, of 15 March, amending Directive no. 2002/58/EC, of 12 June, regulates the retention and transmission of traffic and location data of electronic communications related to natural and legal persons, as well as the related data necessary to identify the subscriber or registered user, for the purposes of investigation, detection, and prosecution of serious crimes by the competent authorities.
II - Directive 2006/24/EC aimed (in the face of major differences in domestic laws that created serious practical difficulties and hindered the functioning of the internal market) to establish harmonisation standards, within the European Union, for the retention of traffic data and location data, as well as the related data necessary to identify the subscriber or registered user, which are standards for the processing of data by communication service providers for a specific purpose, but it did not regulate, nor could it regulate, the activities of public authorities (law enforcement agencies, public prosecutors, judges, and courts) with powers to ensure that this purpose is achieved.
III - It is important to distinguish between the activity of retaining traffic and location data and the activity of accessing that data, as there represent different interferences in terms of fundamental rights, such as the right to privacy.
IV - The framework for access to personal data by competent authorities for the purposes of preventing, investigating, detecting, or prosecuting criminal offences or enforcing criminal sanctions is provided for in Law no. 59/2019, of 08.08 (Personal Data Protection Law), which transposed Directive (EU) 2016/680.

V - Access to data retained by communication service providers within the scope of criminal proceedings is provided for in Articles 187 to 189 and 269(1)(e) of the CPP and by Law no. 109/2009, of 15 September (Cybercrime Law).

VI - Accordingly, as they operate in distinct spheres, Law no. 32/2008, of 17 July, did not repeal, nor could it have repealed, Articles 187 to 189 of the CPP.

VII - The legislator, in Law no. 32/2008, of 17 July, went beyond the transposition of Directive 2006/24/EC, legislating not only on the retention and transmission of data but also on access to this data for use as evidence in criminal proceedings (see Article 9, declared unconstitutional by TC Judgement no. 268/2022). However, this change should have been made in the appropriate place, i.e. in the Code of Criminal Procedure, which was not the case, as the wording of Articles 187(1) and 189(2) remained unchanged. As a result, there is now a catalogue of crimes for which this data could be used as evidence, i.e. the serious crimes provided for in Article 2(1)(g), which is different from the catalogue provided for interceptions in Article 187(1) of the CPP.

VIII - Article 189(2) of the CPP, which was not repealed by Law no. 32/2008, of 17.07, is, therefore, the basic rule for access to traffic and location data retained to prove the offences provided for in Article 187(1) of the CPP that do not fall within the concept of serious crimes in Article 2(1)(g) of that law.

IX - Even if it were not the case, currently, in light of the declaration of unconstitutionality with general binding force of Article 9 of Law no. 323/2008, of 17.07, by virtue of TC Judgement no. 268/2022, taking into account the provisions of Article 282 of the CRP, Article 189(2) of the CPP should always be considered repristinated. This means that, currently, this legal provision would always be the only rule that allows access to retained traffic and location concerning the offences indicated in Article 187(1) of the CPP.

X - The judgement of the Constitutional Court no. 268/2022 left untouched the aforementioned framework of access to data retained by the authorities with a view to investigating certain crimes, namely the aforementioned Articles 187 to 189 of the CPP and the aforementioned Law no. 109/209 (Cybercrime Law).

XI- However, since Law no. 32/2008 has been declared unconstitutional with general binding force, in the sense that has been pointed out, and Directive 2006/24/EC was previously declared invalid (Judgement of 08.04.2014, Digital Rights Ireland), Directive

2002/58/EC of the European Parliament and of the Council of 12.06, transposed by Law no. 41/2004, of 18.08, remains in force.

XII - Law 41/2004, of 18.08, broadly imposes on electronic communications service providers the obligation to retain traffic and location data for billing purposes for a period of 6 months after each communication.

XIII- Although, according to this law, the data retained are not intended to be used as evidence in criminal proceedings, there is nothing to prevent them from being used for that purpose.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRG:2023:12.23.6.PBGMR.A.G1.EE/

- **Judgement of the Guimarães Court of Appeal of 17-10-2023**
  Case no. 308/19.1JAVRL.G1
  Rapporteur: Judge Paulo Almeida Cunha

1. Just as Directive 2006/24/EC did not repeal Directive 2002/58/EC - except for the addition of paragraph 1-A to Article 15 of the latter - Law no. 32/2008 did not repeal Law no. 41/2004 in terms of mere data retention, and now coexists with it, albeit with different scopes of application, namely with regard to the catalogue of relevant crimes and the data retention period.

2. Similarly, in terms of access to retained data, it must be understood that Article 9 of Law no. 32/2008 did not completely repeal Article 189(2) of the CPP, without prejudice to the respective and exclusive derogation in the part relating to the data retained and the extent of the catalogue of relevant crimes

3. The unconstitutionality declared with general binding force the Judgement of the Constitutional Court no. 268/2022 affected the domestic legal framework for the retention and transmission of data generated by electronic communications.

4. With this declaration of unconstitutionality with ex tunc effect, it became unequivocal that mobile communications operators can no longer retain or transmit data under Articles 4 to 6, as well as under Article 9 of Law no. 32/2008.

5. Excluding the application of Law no. 32/2008, the retention of location data by mobile communication operators and their transmission to the judicial authority is fully subject

to the framework already analysed above, as provided for in Article 189(2) of the Code of Criminal Procedure (as amended by Law no. 48/2007), and Law no. 41/2004 of 18 August, in particular Articles 1(2), (4), and (5), Article 2(1)(e), 5, 6(2) and (3), and 7 (as amended by Law no. 46/2012), including the reference made here to the six-month limitation period for the right to receive payment for the services rendered, as provided for in Article 10(1) of Law no. 23/96, of 26 July (as amended by Law no. 24/2008).

6. Due to the repristination effect provided for in Article 282(1) of the Constitution, the declaration of unconstitutionality in question cannot but affect the aforementioned tacit derogation from Article 189(2) of the Code of Criminal Procedure (as amended by Law no. 48/2007) operated by Article 9 of Law no. 32/2008 and, consequently, the provision of Article 189(2) of the Code of Criminal Procedure returns to its scope prior to the entry into force of Law no. 32/2008.

7. Thus, on the one hand, the collection and inclusion in the case file of data on cell location or records of conversations or communications can only be ordered or authorised, at any stage of the proceedings, by order of the judge regarding the crimes provided for in Article 187(1) of the CPP and in relation to persons referred to in paragraph 4 of the same article (Article 189(2) of the CPP).

8. On the other hand, mobile communication operators cam only process and transmit this data during the six months following the provision of the service and must respond to requests for access to personal data from users made by the competent judicial authorities, in particular under the aforementioned Article 189(2) of the CPP and Law no. 41/2004.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRG:2023:308.19.1JAVRL.G1.1F/