SUPREMO TRIBUNAL DE JUSTIÇA *(SUPREME COURT OF JUSTICE)*

NATIONAL CASE LAW

PERSONAL DATA PROTECTION

REGULATION (EU) 2016/679, OF THE PARLIAMENT AND OF THE COUNCIL OF 27.04.2016

LAW NO. 58/2019, OF 08.08

JANUARY 2024 TO DECEMBER 2024

COLLATED BY:

CÁTIA COSTA SANTOS

(JUDGE ADVISOR TO THE SUPREME COURT OF JUSTICE)

I. CONSTITUTIONAL COURT

- **Judgement of the Constitutional Court no. 533/2024 of 04-07-2024**

  Rapporteur: António José de Ascensão Ramos

  Decision:

"In these terms and on these grounds, it is decided:

a) Not to deem unconstitutional the provisions of Article 18(1)(c) of Law 19/2012 of 8 May (in its original wording, prior to that conferred by Law 17/2022 of 17 August), when interpreted:

i) - In the sense that "it is possible, in competition offence proceedings, to examine, collect and seize e-mail messages";

ii) - To admit the "possibility of examining, collecting and/or seizing "open" or "read" e-mails";

iii) - To "allow the examination, collection and seizure of e-mails in competition offence proceedings without a prior court order";

https://www.tribunalconstitucional.pt/tc/acordaos/20240533.html

- **Judgement of the Constitutional Court no. 426/2024 of 29-05-2024**

  Rapporteur: Maria Benedita Urbano

  Decision:

"In view of the above, it is decided:

a) Not to deem unconstitutional the interpretation of the provisions of Article 64(1) and (2)(e) of the General Tax Law, approved by Decree-Law no. 398/98, of 17.11 and as amended by Law no. 83-C/2013, of 31.12, of Article 6(5)(b) and (9) of the Law on Access to Administrative Documents - Law no. 26/2016, of 22.08, as amended by Law no. 58/2019, of 08.08, to the effect of sealing Article 130(1) of the Municipal Property Tax Code, approved by Decree-Law no. 287/2003, of 12.11, in the sense of prohibiting

access to the address of the owner registered in the rustic property matrix, when requested by indicating the article number of the matrix and when the building is not registered, and, consequently,

b) Reject as unfound the present constitutionality appeal".

https://www.tribunalconstitucional.pt/tc/acordaos/20240426.html

- **Judgement of the Constitutional Court no. 506/2024 of 28-06-2024**

  Rapporteur: José Teles Pereira

  Decision:

"In view of the above, it is decided:

a) not to rule unconstitutional the rule contained in Article 125 of the Code of Criminal Procedure, when interpreted to mean that it is permissible to value the data collected by a GPS installed in a vehicle by its owner, handed over by the latter at the request of the Judicial Police for the purposes of criminal investigation; consequently,

b) reject as unfound the appeal as to the rule indicated in the previous paragraph;

c) to declare unconstitutional the rule contained in Article 125 of the Code of Criminal Procedure, when interpreted to mean that the addition to a criminal case of data collected by a GPS installed in a vehicle by its owner, delivered by the latter at the request of the Judicial Police for the purposes of criminal investigation, does not require validation by a judge, for violation of the provisions of Articles 26(1) and 18(2) of the Constitution of the Portuguese Republic; consequently,

d) uphold the appeal as regards the unconstitutionality of the rule referred to in the preceding paragraph, and order that the case be referred to the Supreme Court of Justice so that it may reform its decision in accordance with this judgement of unconstitutionality; and

e) not to take cognisance of the subject matter of the appeal in relation to the other issues raised by the appellant."

https://www.tribunalconstitucional.pt/tc/acordaos/20240506.html

- **Judgement of the Constitutional Court no. 852/2024 of 05-12-2024**

  Rapporteur: Joana Fernandes Costa

  Decision:

"*For the reasons set out above, it is decided:*

a) Not to rule unconstitutional the rule in Article 4(3) and (5) of Law 113/2009 of 17 September, according to which, in the case of employment, profession or activity involving regular contact with minors, the request for provisional cancellation of a decision to sentence the applicant to a fine for committing a crime of sexual harassment, provided for in Article 170 of the Penal Code, against a person of legal age, can only be granted if a psychiatric examination is carried out, with the intervention of three specialists, with a view to assessing the applicant's rehabilitation, even if the Sentencing Court, in a reasoned order, deems it manifestly unnecessary in the case; and, consequently,

b) Grant the appeal filed by the Public Prosecutor's Office, ordering that the contested decision be reformed in accordance with this negative judgement of unconstitutionality."

https://www.tribunalconstitucional.pt/tc/acordaos/20240852.html

II. SUPREME COURT OF JUSTICE

- **Judgement of the Supreme Court of Justice of 31-01-2024**

  Process: no. 170/11.2TAOLH-E.S1

  Rapporteur: Counsellor Lopes da Mota

I. Under the terms of Article 449(1)(f) of the CCP, review of a final judgement is admissible when the Constitutional Court ("TC") declares the unconstitutionality, with general binding force, of a rule less favourable to the defendant that served as the basis for the conviction. In an interpretation that conforms to the Constitution (Article 282(3)), a review can only take place on this basis when the Constitutional Court makes a decision that goes against the constitutionally imposed res judicata proviso; if there is no decision

to the contrary, all res judicata that applied the rule declared unconstitutional remain untouched.

II. The rules of Law no. 32/2008, of 17 July, which the Constitutional Court declared unconstitutional in judgement no. 268/2022, with general binding force, concern 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 related data necessary to identify the subscriber or registered user, for the purposes of investigation, detection and prosecution of serious crimes, as defined in national law, by the competent national authorities.

III. The data processed and stored is data relating to communications, in their various forms of realisation, with each record beginning with the establishment of the communication and ending with its termination; this excludes data which, although it may be identical, has not been processed in relation to communications made, such as data relating to the identification of subscribers obtained and processed in the context of the contractual relationship with the service provider.

IV. Law 32/2008 transposes into national law Directive no. 2006/24/EC of 15 March, amending Directive 2002/58/EC of 12 June, adopted on the basis of Article 95 of the Treaty establishing the European Community (which concerned the functioning of the internal market, formerly the 1st pillar of the Union).The main aim of this directive was to harmonise the provisions of the Member States concerning the obligations of providers of electronic communications services or public communications networks to ensure the retention of such data, by way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, which transposed the principles laid down in Directive 95/46/EC (transposed into national law by Law 67/98 of 26 October, replaced by the GDPR) into rules specific to the electronic communications sector.

V. Article 15(1) of Directive 2002/58/EC, transposed into national law by Law 41/2004, of 18 August, which remains in force, provides that, to that end, member states may adopt legislative measures and lists the conditions for restricting confidentiality and prohibiting the storage of traffic and location data (“metadata”), but it is not applicable to the state's activities in criminal matters, which was an area of intergovernmental cooperation (formerly the 3rd pillar of the Union).

VI. A distinction must be made between data retention operations, regulated by "Community law" rules (former 1st pillar) and data access operations, regulated by national criminal procedural rules and the former 3rd pillar of the Union (a distinction that must be maintained after the Lisbon Treaty, with the abolition of the "pillarisation" of Maastricht).These 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 personal data protection, which, subject to the principles, are subject to restrictions necessary for the protection of other rights, in particular the right to liberty and security.

VII. It is for national law to determine the conditions under which service providers must grant the competent national authorities access to the data in their possession, in the context of criminal proceedings, for the purpose of investigating and prosecuting serious crime, with due regard for the essential principles and rules of criminal procedure, in particular the principles of proportionality, prior review by a court, adversarial proceedings and due process (see CJEU judgements of 21.12.2016, *Tele2 Sverige AB*, process C-203/15; of 6.10.2020, *La Quadrature du Net and Others, process* C-511/18, C-512/18 and C-520/18; of 2.3.2021, *H.K. and Prokuratuur*, process C-746/18; and of 5.4.2022, *G.D. and Commissioner of An Garda Síochána and Others*, process C-140/20).

VIII. Access to personal data by the competent authorities, as a data processing operation for the purposes of the prevention, investigation, detection or prosecution of 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 national law by Law no. 59/2019 of 8 August.

IX. Since the retention of data for the purposes of criminal investigation in relation to serious offences, as defined by national law, is permitted by Article 15(1) of Directive 2002/58/EC (and Law 41/2004, which transposes it), Directive 2006/24/EC aimed, in the face of major differences in national laws that were creating serious practical difficulties and difficulties in the functioning of the internal market, to establish harmonisation rules within the European Union for the storage of traffic data and location data, as well as

related data - which are rules that determine the purpose for which data is processed (respect for the principle of purpose, one of the principles that, along with the principles of legality, necessity and proportionality, govern the processing of personal data) - but it did not regulate, nor could it regulate, the activity of public authorities (criminal police bodies and judicial authorities - the Public Prosecutor's Office, judges and courts) with the power to ensure the fulfilment of that purpose through criminal proceedings.

X. In a different dimension, Law 32/2008 did not repeal or establish rules of a criminal or criminal procedural nature, which the judicial authorities must use to access and acquire evidence or to ensure its validity in the proceedings; such activities have their own regime defined by national criminal and criminal procedural laws and, with regard to the areas of competence of the European Union (EU) in the area 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 TFEU and Directive (EU) 2016/680 of the European Parliament and of the Council, transposed by Law 59/2019 of 8 August.

XI. Obtaining data held by communications service providers in criminal proceedings is regulated by other legal provisions: Articles 187 to 189 and 269(1)(e) of the CCP and Law no. 109/2009 of 15 September (the Cybercrime Law), which transposes Framework Decision 2005/222/JHA of 24 February on attacks against information systems into national law and adapts national law to the Council of Europe Convention on Cybercrime (Budapest, 2001), ratified by Portugal.

XII. The Constitutional Court has not declared that the effects of the declaration of unconstitutionality with general binding force under the terms of judgement no. 268/2022 extend to res judicata, under the terms of Article 282(3) of the Constitution, so this declaration of unconstitutionality does not constitute grounds for review of the judgement under Article 449(1)(f) of the CCP.

XIII. The declaration of invalidity of Directive 2006/24/EC by the Court of Justice of the European Union (CJEU), by judgement of 08.04.2014, in references for a preliminary judgement under Article 267 of the TFEU (in the joined cases *Digital Rights Ireland Ltd* (C-293/12) and *Michael Seitlinger* (C-594/12), prior to the judgement in which the appellant was convicted, does not constitute grounds for review of the judgement referred

to in Article 449(1)(g) of the Code of Criminal Procedure (CCP), according to which review is admissible when "a judgement binding on the Portuguese State, handed down by an international body, is irreconcilable with the conviction or raises serious doubts as to its fairness".

XIV. Apart from the fact that the law requires it to 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 precept, which was designed for the decisions of the European Court of Human Rights (bearing in mind Article 46(1) of the ECHR).

XV. A judgement by the CJEU which, in a preliminary judgement appeal, declares a directive invalid under Article 267 TFEU is only addressed directly to the court which referred the matter to the CJEU; the fact that the CJEU's decision constitutes sufficient reason for any other court to consider such an act invalid, as a result of the general obligation to guarantee the primacy of EU law by refraining from taking contrary acts which jeopardise its effectiveness (in this sense one can speak of an *erga omnes* effectiveness - see the CJEU judgement C-66/80 of 13.5.1981), does not give it the status of a procedural subject to which that decision is addressed, so that it should be considered a binding judgement on the basis of the review.

XVI. Therefore, since there are no grounds, the review of the judgement is denied.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:STJ:2024:170.11.2TAOLH.E.S1.B3/

- **Judgement of the Supreme Court of Justice of 21-02-2024**

  Process: no. **966/14.3JAPRT-C.S1**

Rapporteur: Counsellor Lopes da Mota

I. Under the terms of Article 449(1)(f) of the CCP, review of a final judgement is admissible when the Constitutional Court ("TC") declares the unconstitutionality with general binding force of a rule less favourable to the defendant that served as the basis for the conviction.

II. The basis of the appeal is not, in this case, the unconstitutionality of a rule applied in the proceedings that led to the conviction, which finds its space and place for discussion in those proceedings, with the exhaustion of ordinary appeals, which are always

admissible (Article 399 of the CCP), a prerequisite for the admissibility of an appeal to the Constitutional Court, in accordance with the model for monitoring constitutionality established by the Constitution and developed in Law no. 28/82, of 15 November.

III. Without ever invoking it, the appellant invokes reasons that led the Constitutional Court to declare the unconstitutionality with general binding force, by judgement no. 268/2022 of 19.04.2022, of rules of articles 4 and 9 of Law no. 32/2008, of 17 July, for allegedly reconducting the provision of Article 449(1)(f) of the Code of Criminal Procedure (CCP) in isolation and in connection with Article 449(1)(e) of the Code of Criminal Procedure (CCP), because this allegedly also resulted in a conviction based on "prohibited evidence" (Articles 125 and 126 of the Code of Criminal Procedure).

IV. Even if it could be argued that the data that led to the conviction can be identified with the data specified in articles 4 of Law 32/2008, the use of this data would be protected by the res judicata exception, since the Constitutional Court has not declared that the effects of the declaration of unconstitutionality extend to res judicata, under the terms of Article 282(3) of the Constitution, and since the rules declared unconstitutional are not criminal in nature and form part of the *ratio decidendi* of the convicting judgement, it would not be possible to make such an extension.

V. The claim that the conviction was based on "prohibited evidence" - or rather, on the "discovery", subsequent to the conviction, that "evidence prohibited under Article 126(1) to (3)", as required by Article 449(1)(e) of the Code of Criminal Procedure, - cannot stand, on the assumption that it would be the result of the declaration of unconstitutionality, which could constitute an autonomous ground for review, which, however, has not been invoked.

VI. The alleged basis for the conviction on the basis of "prohibited evidence", which did not occur, could only be questioned in the presence of a violation by the judicial authorities of the rules on the acquisition of evidence (Article 126(3) of the CCP), when it was subsequently discovered, which also did not occur.

VII. If there are no grounds and there is a manifest lack of grounds, the review is denied and the sanction referred to in the final part of Article 456 of the CCP is applied.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:STJ:2024:966.14.3JAPRT.C.S1.EE/

- **Judgement of the Supreme Court of Justice of 28-02-2024**

  Process: no. 1044/18.1T9EVR.E1.S1

  Rapporteur: Counsellor Ana Barata Brito

I. The offence of violating the rules on files and forms set out in Article 43(1) of Law 37/2015 is committed by transferring a CRC (*criminal record certificate*) containing confidential information and issued to be attached to a specific case to another case, causing this transfer to take place without the data subject's knowledge or the decision of the competent judicial authority.

II. Given the favourable personal conditions of the defendant and the other circumstances - a lawyer with a good work, family and social background, no criminal record, no specific intention to harm the assistant's honour and dignity, but rather to act in the interests of his client, disclosure of the document in the strict judicial context, subsequent behaviour - a low degree of guilt justifies the application of a penalty of admonishment.

III. The reasons that justify opting for a penalty of admonition rather than a fine also justify granting the other claim made in the appeal, that the conviction should not be entered on the criminal record certificate, a matter that the Supreme Court can decide immediately, since in this procedural framework of total consensus and given the meaning of the decision to be handed down, there would always be no right to appeal to be safeguarded.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:STJ:2024:1044.18.1T9EVR.E1.S1.A5/

III. COURTS OF APPEAL

LISBON COURT OF APPEAL

- **Judgement of the Lisbon Court of Appeal, of 09-01-2024**

  Process no. 1526/19.8TELSB-F.L1-5

  Rapporteur: High Court judge Ana Cláudia Nogueira

I- The general rule of procedure in the execution of the seizure of assets in criminal proceedings is that seals must be affixed to the seized objects, under the general terms provided for in Article 184 of the Code of Criminal Procedure, and this is only dispensed with when it is not possible; failure to affix seals, when possible, constitutes a procedural irregularity under the regime provided for in Article 123 of the Code of Criminal Procedure.

II- The Cybercrime Law approved by Law 109/2009, of 15/09 provides under Article 16/7 a special procedure for executing the seizure of computer data or documents which, "depending on whether it is more appropriate and proportionate, taking into account the interests of the specific case, may, in particular, take the following forms:

a) Seizure of the medium on which the system is installed or seizure of the medium on which the computer data is stored, as well as the devices needed to read it;

b) Making a copy of the data, on a separate medium, which will be attached to the file;

c) Preservation, by technological means, of the integrity of the data, without copying or removing it; or

d) Non-reversible deletion or blocking of access to data.".

III- In this special procedure, sealing is only provided for in the case of a seizure carried out under the terms of paragraph b), with seals being affixed to the copy of the seized data to be entrusted to the judicial secretary of the services where the proceedings are taking place - Article 16(8) of the Cybercrime Law.

IV- The primary purpose of affixing seals is to guarantee the safety of seized goods and preserve their evidential value.

V- However, in particular situations, signalled by the legislator through the establishment of special search and seizure regimes, depending on the sensitivity of the interests at stake, whether due to the object of the seizure or the specific locations where the seizure takes place, the affixing of seals can also function as a way of protecting the secrecy to which the seized goods are subject and the privacy of private life.

VI- This is the case with the seizure of correspondence - Article 179 of the Code of Criminal Procedure - which also applies to electronic correspondence through the reference made in Article 17 of the Cybercrime Law, and the seizure of goods that may conflict with commercial, industrial or so-called business secrets, under the terms of articles 318, 331 and 352 of Decree-Law 110/2018, of 10 December, which approved the Industrial Property Code.

VII- If there are documents that are relevant to the evidence to be added to the case file, given the rule of publicity in criminal proceedings laid down in Article 86/1 of the Code of Criminal Procedure, they must comply with the legal rules on secrecy, adopting all the procedures laid down by law, and others that are deemed necessary, to safeguard the various secrets that may be involved, but also the privacy of private life.

VIII- In the course of the enquiry, it is up to the Public Prosecutor's Office, its holder, of its own motion or at the request of the interested parties, to adopt these procedures, and specifically those provided for in Article 352 of Decree-Law 110/2018, of 10 December, which approved the Industrial Property Code, aimed at preserving the confidentiality of trade secrets in legal proceedings, which may include the creation of a confidential annex excluded from consultation by third parties unrelated to the proceedings.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2024:1526.19.8TELSB.F.L1.5.AE/

- **Judgement of the Lisbon Court of Appeal, of 09-01-2024**

  Process no. 152/22.9T9VLS.L1-5

  Rapporteur: High Court judge Ana Cláudia Nogueira

I. The administrative decision in administrative offence proceedings is not subject to the same formal requirements as a judicial decision, but follows the regime specifically laid down in Article 58 of the General Regime of Administrative Offences approved by Decree-Law 433/82 of 27 October;

II. Although the administrative decision must contain a description of the facts charged, with an indication of the evidence obtained, as well as an indication of the rules according to which it is punished and the grounds for the decision, it is not required that these grounds include a *critical examination of the evidence* that served to form the conviction

of the administrative authority, contrary to what is expressly enshrined for the judgement in Article 374/2 of the Code of Criminal Procedure.

III. As this is an administrative phase, subject to the characteristics of procedural speed and simplicity, the duty to state reasons should be qualitatively less intense than that required for a criminal judgement; the point is that the decision should clearly state the reasons in fact and in law that led to the conviction, making it possible for the defendant to attack its grounds and defend himself against it, namely in court challenges, but also allowing the court to know the logical process of forming the conviction.

IV. Since June 2013, with the entry into force of Law 34/2013, of 16/05, by means of its Article 8/3 and 4, fuel supply establishments have been legally obliged to install video surveillance systems with recording and preservation of images for a period of 30 days - Article 31/2.

V. As follows from the provisions of Article 8/4, with reference to paragraph 3, both of Law 34/2013, of 16/05, this obligation does not fall on the companies contracted by the owners of these petrol stations to install video surveillance systems and technical assistance, but on those who own and operate these same stations.

VI. Although the technical operation of installing, maintaining and servicing the video surveillance system can only be carried out by entities with a permit or licence to exercise private security - articles 3/1, 2, c) and 14/1, 2, c) and 4, of Law 34/2013, of 16/05 -, the owner of the petrol station where this system is installed still has access to it, and can intervene in it using that technical support in order to enforce the legal requirements, namely those relating to image recording and preservation.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2024:152.22.9T9VLS.L1.5.1B/

- **Judgement of the Lisbon Court of Appeal, of 11-01-2024**

  Process no. 4551/22.8T8FNC-A.L2-2

  Rapporteur: High Court judge Higina Castelo

I. It is admissible for the landlady to attach her bank account statements to the case file, in order to prove the alleged payment of rents that the tenant should have made by deposit in the same account, even if these statements contain third party data.

II. A person who claims to be in bad faith relies on rent receipts that he knows were issued in error, as they correspond to rents that he did not pay, as he well knows. https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2024:4551.22.8T8FNC.A.L2.2.7A/

- **Judgement of the Lisbon Court of Appeal, of 23-01-2024**
  Process no. 143/17.1JGLSB.L1-5
  Rapporteur: High Court judge Sara André Marques

I- Article 68(1) of the CCP must be interpreted in a systematic way, conferring legal standing to be an assistant in semi-public crimes only on the offended party who has exercised the right to complain.

II- Article 194 of the Penal Code protects (formal) privacy, in the sense of the "right to communicative self-determination", while also protecting, in a reflexive and derivative way, interests of a supra-individual nature, such as the inviolability of correspondence and telecommunications.

III- In the case of emails, the legal and criminal protection provided by Article 194 persists as long as the message remains in the mailbox, without being definitively stored anywhere on the recipient's computer and deleted from the provider's servers, as it remains under the control of the electronic service provider.

IV- Legal persons have the right to privacy.

V- Legal persons have the right to complain when it comes to the dissemination of constant emails, from hidden mailboxes, in a legal person's domain, sent and received by employees in the interest and on behalf of this.

VI- The invasion of correspondence and telecommunications is only permitted in the cases provided for in Article 34(4) of the Constitution of the Portuguese Republic, therefore, the justification of exercising the right to inform and the right to free expression, under the terms of Article 31 of the Penal Code, cannot be invoked to justify the disclosure of emails from violated mailboxes.

VII- There is a collective feeling that the right to inform ceases in the face of the inviolability of communications.

VIII- A published book is a "media outlet", under the terms and for the purposes of Article 183(2) of the Penal Code.

IX- In the case of the offence provided for in Article 187 of the Penal Code, the cause of justification provided for in Article 180(2) of the Penal Code does not apply.

X- The rules establishing the causes of suspension of the limitation period for criminal proceedings introduced by Article 6-B, paragraph 3 of Law no. 4-B/2021, of 1 February, which came into force without changes from 22 January 2021 (Article 4 of Law no. 4-B/2021) until 5 April 2021 (Article 7 of Law no. 13-B/2021), apply to cases pending on the date of their entry into force.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2024:143.17.1JGLSB.L1.5.C1/

- **Judgement of the Lisbon Court of Appeal, of 25-01-2024**

  Process no. 13467/21.4T8LSB.L1-2

  Rapporteur: High Court judge Carlos Castelo Branco

I) The inclusion in the case file of the document proving that the patron appointed under the legal aid scheme has asked to be excused from the case interrupts the period in progress, which will begin to run in full from the date of notification of the decision assessing the excusal - see articles 34(2) and 24(5) of Law 34/2004 of 29 July (Law on Access to Law and the Courts), as amended by Law 47/2007 of 28 August.

II) Since the appellant's challenge to the facts lacks an express position on the outcome sought and on the specific points of fact considered to have been incorrectly judged - and therefore fails to comply with the burden of challenge set out in Article 640(1)(a) and (c) of the Code of Civil Procedure - the challenge to the facts must be rejected.

III) The right to "erasure of data", provided for in Article 17(1) of the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 or GDPR) fulfils one of the main objectives of the GDPR, namely to ensure a high level of data protection by giving the holders of personal data effective power over their own data, recognising their right to control personal data and to delete data if the holder so wishes, namely when the purposes for which they were collected have been achieved.

IV) If the right to erasure is exercised, the controller is obliged to erase the personal data without undue delay, in particular when the data subject withdraws the consent on which the processing of their data was based and if there is no other legal basis for continuing to process the data.

V) The *"right to erasure"* will not apply, *"insofar as the processing proves necessary:*

a) To the exercise of freedom of expression and information;

b) To the fulfilment of a legal obligation requiring processing provided for by Union or Member State law to which the controller is subject, the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

c) For reasons of public interest in the field of public health, under the terms of Article 9(2)(h) and (i), as well as Article 9(3);

d) For archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes pursuant to Article 89(1), in so far as the right referred to in paragraph 1 is likely to render impossible or seriously jeopardise the achievement of the objectives of such processing; or

e) For the purposes of declaring, exercising or defending a right in legal proceedings" (see Article 17(3) of the GDPR).

VI) Since it has been shown that the plaintiff carried out operations with the loyalty card in the 1st defendant's shops until at least March 2017 (purchasing tickets - purchases and sales), the 1st defendant is entitled to retain the data relating to the plaintiff, due to the establishment of such legal relationships and the consequences arising from them, if, namely, the legal obligations determining such retention remain in force.

VII) Under the terms of Article 21 of Law no. 58/2019, of 8 August, *"the period of retention of personal data is that fixed by law or regulation or, in the absence thereof, that which is necessary for the pursuit of the purpose"* (no. 1), and *"in cases where there is a period of retention of data imposed by law, the right to erasure provided for in Article 17 of the GDPR may only be exercised at the end of that period"* (no. 5).

VIII) Article 125(1) of the Corporate Income Tax Code establishes that *"taxable persons with registered offices or effective management in national territory, as well as those with a permanent establishment there, are subject to the obligations of invoicing and keeping books, records and respective supporting documents under the terms of the VAT Code*

and Decree-Law no. 28/2019 of 15 February" - and Article 52(1) of the Value Added Tax (VAT) Code establishes that "taxable persons are obliged to file and keep in good order for the following 10 calendar years all books, records and their supporting documents, including, when the accounts are kept by computerised means, those relating to the analysis, programming and execution of processing", and Article 19(1) of Decree-Law no. 28/2019 of 15 February (amended by Decree-Law no. 48/2020 of 3 August), *"taxable persons are obliged to file and keep in good order all books, records and respective supporting documents for a period of 10 years, if no other period results from a special provision"*-, the 1st defendant currently retains the right to keep documents relevant for tax purposes, since the respective retention periods for tax documents have not yet elapsed since the date of the business transactions with the plaintiff (the last on 25 March 2017) and, consequently, it is entitled to keep - by processing - the plaintiff's personal data, without the plaintiff being able to successfully assert the right to erasure of such data.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2024:13467.21.4T8LSB.L1.2.61/

- **Judgement of the Lisbon Court of Appeal, of 25-01-2024**
  Process no. 1/21.5ICLSB-A.L1-9
  Rapporteur: High Court judge Fernanda Sintra Amaral

I. The legislator of the Cybercrime Law, with the reference in Article 15(1) to obtaining specific and determined computer data, certainly did not intend to include a legal requirement for the exact and rigorous pre-identification of the computer data to be searched in the course of searches, but only intended there to be an interconnection between the computer data searched and its evidential relevance to the discovery of the material truth.
II. The procedure that has been generically referred to as "blind copying" is not, in itself and immediately, reprehensible or inadmissible, and the need to search for computer data (Article 15 of the Cybercrime Law), in an external location, may be justified in relation to the location searched, by resorting, exceptionally, to the "blind copying" of such files.
III. The fact is that the "blind copy", which was only used because of the large size of the files to be searched, is not a seizure in the strict sense, but rather a necessary preliminary

step, a merely "facilitating" action, with a view to allowing extensive work to be done afterwards: carrying out the search duly authorised by the Investigating Judge (JIC) - which, due to the exceptional circumstances mentioned, will have to take place in an external location.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2024:1.21.5ICLSB.A.L1.9.E7/

- **Judgement of the Lisbon Court of Appeal, of 18-04-2024**

  Process no. 28507/23.4 T8LSB.L1-8

  Rapporteur: High Court judge Teresa Sandiães

- The exception provided for in Article 127(3)(a) of EU Regulation 2016/679 of 27 April 2016 presupposes that the processing of personal data is necessary for the exercise of freedom of expression and information. In other words, the exception does not apply automatically, requiring a balance between, on the one hand, the fundamental rights to respect for private life and the protection of personal data, enshrined in Articles 7 and 8 of the Charter of Fundamental Rights, and, on the other, the fundamental right to freedom of information, guaranteed by Article 11 of the Charter.
- The news item/content dates back to 2001, concerns events that took place more than 20 years ago, the applicant is not a public figure, she was acquitted of the crime of homicide by negligence that she was accused of in the exercise of her profession as a doctor, to which the accusation conveyed by the news item/content referred, no social alarm arouses such an accusation, given the outcome of the trial. She is not being accused of exercising functions with media exposure or playing an administrative or political decision-making role. There is no question of acting in a public place (possibly implying greater exposure).
- In view of these circumstances, the disclosure of this content on the internet is of no current public interest and causes serious damage to the applicant's personality rights (good name, image and personal and professional reputation). Therefore, in terms of a proportionality judgement, since such disclosure is absolutely unnecessary for the exercise of freedom of information, the applicant's right to be forgotten prevails, through

the elimination/deletion of the news/content, since the exception provided for in Article 17(3)(a) of the Regulation is ruled out.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2024:28507.23.4.T8LSB.L1.8.97/

- **Judgement of the Lisbon Court of Appeal, of 09-05-2024**

  Process no. 6308/22.7T8VNG-B.L1-6

  Rapporteur: High Court judge Adeodato Botas

1- The order directing a party to attach certain documents in order to allow for the assessment of dilatory exceptions, or the knowledge, in whole or in part, of the merits of the case in the final judgement, is legally based on Article 590(2)(c), and constitutes a binding order for the judge and not a decision made using discretionary power.

2- And because it is a decision on evidence, even if it is made of its own motion, that order is immediately and autonomously appealable, under the terms of Article 644(2)(d) of the Code of Civil Procedure.

3- If the document ordered to be produced contains personal details of the plaintiff's associates, the court must determine that access to the file is limited, taking into account the provisions of Article 164(3) of the Code of Civil Procedure and Law 58/2019 of 08/08, as well as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2024:6308.22.7T8VNG.B.L1.6.1D/

- **Judgement of the Lisbon Court of Appeal, of 21-05-2024**

  Process no. 3363/22.3T8OER.L1-7

  Rapporteur: High Court judge Luís Filipe Pires de Sousa

I. With regard to the publication of images and/or texts about private life, the ECtHR (*European Court of Human Rights*) has essentially identified the following criteria for gauging the balance of competing rights:

i. Contribution to a debate in the public interest;

ii. The degree of notoriety of the person affected;

iii. The subject of the report;

iv. The previous behaviour of the person concerned;

v. The content, form and consequences of publication;

vi. The way in which the information was obtained and its veracity;

vii. If applicable, the circumstances in which the photographs were taken.

II. The circumstances of the case may determine that certain criteria are more or less relevant.

III. The ECtHR's case law enshrines the criterion of public interest in knowing the facts, and it is not permitted to capture the image of public figures if, even if they are in public places, they are not directly or indirectly exercising functions for which they have become known.

IV. The mistakes of the past (addiction to alcohol) do not have to be a permanent sword of Damocles over the author's head, especially when it shows a purpose of personal improvement, and the plaintiff has the right to rehabilitation, which is made difficult by the permanent reminder of the past addiction.

V. The fact that the photographs were taken when the plaintiff was on the public highway does not mean that they relate to the public sphere of the plaintiff 's life.

VI. According to the ECtHR, the public interest cannot be reduced to the public's thirst for information about the private lives of others or to the reader's desire for sensationalism or voyeurism.

VII. The discussion of the author's addiction to alcohol would only be legitimate as a matter of public interest if the specific situation of drunkenness had occurred or manifested itself in the author's work environment. In fact, the assessment of public interest in this context requires that the act or conduct revealed have a connection with or produce effects on the activity of the public figure, which is not the case here.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2024:3363.22.3T8OER.L1.7.75/

- **Judgement of the Lisbon Court of Appeal, of 04-06-2024**

  Process no. 41/24.2JBLSB-A.L1-5

  Rapporteur: High Court judge Maria José Machado

I – Article 6(2) of Law no. 32/2008, of 17 July, introduced by Law no. 18/2024, of 5 February, excepts from the retention regime provided for therein, the retention of data by the entities provided for in Article 4(1), under the terms defined contractually with the client for the purposes arising from the respective commercial legal relationships, which includes the billing data provided for in Law no. 41/2004, of 18 August, or by virtue of a special legal provision.

II - The traffic data for billing purposes that companies providing electronic services can store for six months is, in itself, a valid and legal means of evidence that the Public Prosecutor's Office can use for investigation purposes, particularly when a serious crime is involved and this evidence is indispensable for discovering the truth. Such data is not subject to the retention regime laid down in Article 6(2) of Law 34/2008, any more than traffic and location data that is retained under a special legal provision, such as the cybercrime law, so that it can be passed on for investigative purposes.

III - There is no legal obstacle to the fact that, if the investigation of a serious crime is in question and such data is indispensable for discovering the truth, as is the case here, the Public Prosecutor's Office cannot request the investigating judge to transmit it to the company providing the electronic services in question, under the terms of Article 9 of Law no. 34/2008, as long as such traffic data is only that which the company can keep for six months for billing purposes and without the need for such data to have been retained under the terms of Article 6(2) of Law 34/2008.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2024:41.24.2JBLSB.A.L1.5.C8/

- **Judgement of the Lisbon Court of Appeal, of 24-10-2024**

  Process no. 2495/22.1T8LSB.L1-6

  Rapporteur: High Court judge Gabriela de Fátima Marques

I. Although the defendant is not a media organisation, this does not prevent it from indexing content that contributes to the exercise of freedom of expression and information by citizens.

II. The right to erasure, as provided for in Article 17 of the General Data Protection Regulation (GDPR), does not apply if there are overriding legitimate interests, namely

the exercise of freedom of expression and information, and both the interests of the person responsible and those of third parties may be at stake.

III. In order to weigh up the right to respect for private life against the right to freedom of expression and information, a number of relevant criteria must be taken into account, such as the contribution to a debate of general interest, the degree of notoriety of the person affected, the subject of the report, the previous behaviour of the person concerned, the content, form and consequences of the publication, the manner and circumstances in which the information was obtained, as well as its veracity.

IV. However, as to whether they are true or not, a distinction must be made between statements of fact and judgements of value, because while the materiality of the former can be proven, the latter do not lend themselves to a demonstration of their accuracy.

V. When the person concerned plays a role in public life, that person must show an increased degree of tolerance, since they are inevitably and knowingly exposed to public scrutiny.

VI. In this case, the expressions used by the author of the blog cannot even be objectively considered offensive to the Appellant's honour and good name, since, according to the general feeling of the community, it is unreasonable to consider that these, in the context in which they were uttered, deserve any judgment of censure, but rather consist of mere opinions.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2024:2495.22.1T8LSB.L1.6.D8/

- **Judgement of the Lisbon Court of Appeal, of 05-11-2024**
  Process no. 1016/21.9PSLSB.L1-5
  Rapporteur: High Court judge Sandra Oliveira Pinto

I- The investigative decision is concerned with the assessment of all the (indicative) evidence produced in the investigation and pre-trial proceedings and its integration and legal framework, in order to assess whether or not it is sufficient to justify putting the defendant on trial for the offence that the assistant accuses him of. In making this judgement, the court assesses the evidence according to the rules of experience and its own free judgement (Article 127 of the Code of Criminal Procedure).

II- Since the defendants are employees in the service of a public employer, such as the Tax Authority, they are bound by the duty of obedience, which consists of following and complying with the orders of legitimate hierarchical superiors, given in the course of duty and in the legal form (see Article 73(1), (2)(f) and (8) of the General Public Employment Law, approved by Law 35/2014 of 20 June, applicable by express reference to Article 49 of Decree-Law 132/2019, of 30 August - which establishes the regime of the special career of tax and customs management and inspection and the special career of tax and customs inspection and audit of the Tax and Customs Authority (AT), as well as tax and customs managers) - which is what they did in this case, as the case file documents.
III- As a direct result of Article 32(2) of the Constitution of the Portuguese Republic, all criminal proceedings are based on the principle of the presumption of innocence, from which also derives the accusatory structure of criminal proceedings (paragraph 5 of the aforementioned Article 32), with the consequence that it is always up to the accuser to demonstrate the verification of the assumptions on which the existence of criminal liability depends, in order to overcome the aforementioned presumption of innocence.
IV- The sufficiency of the evidence contains the same requirement of truth required for the final judgement, but it is assessed in the light of the probative and convicting elements contained in the investigation (and pre-trial investigation) which, by their nature, could possibly allow a judgement of conviction that will not be confirmed at trial; however, if at this level of judgement on the facts it is not possible to foresee the likelihood of a future conviction, the evidence is not sufficient, and there is not enough proof for the charge (or for the indictment).
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2024:1016.21.9PSLSB.L1.5.E4/

- **Judgement of the Lisbon Court of Appeal, of 21-11-2024**
  Process no. 85/18.3TELSB-F.L1-9
  Rapporteur: High Court judge Maria de Fátima R. Marques Bessa

I. The Cybercrime Law, Law no. 109/2009 of 15 September, transposed into national law Council of Europe Framework Decision no. 2005/222/JHA of 24 February on attacks against information systems and adapts national law to the Council of Europe Convention

on Cybercrime adopted in Budapest on 23 November 2001 (approved by Assembly of the Republic Resolution no. 88/2009 of 10 July 2009 published in the Official Gazette, I series of 15 September 2009 and ratified by Decree no. 91/2009 of 15 September).

II. Law no. 109/2009 established for the first time specific legal rules (substantive and procedural criminal provisions) regarding the collection of evidence on electronic media, and under the terms of Article 11(1), the provisions contained therein are applicable to any and all criminal offences, provided that the collection of evidence on electronic media is necessary, and Articles 15 to 17 contain regulations on the search (Article 15) and seizure of data or computer documents previously stored in a computer system (articles 16 and 17), establishing a special regime for the seizure of electronic mail and communications records of a similar nature.

III. As a rule, it is the competent judicial authority - the Judge or the Public Prosecutor's Office - who, depending on the procedural stage, authorises or orders the search and seizure whenever it is indispensable for the evidence (Article 16(1)).

IV. The law individualises two specific situations whose sensitivity and legal-constitutional relevance justifies the provision of a particular regulatory regime relating to the seizure of sensitive data (personal or intimate data that could jeopardise the privacy of the data subject or third parties) (Article 16) and electronic mail and records of a similar nature (Article 17).

V. It follows from Article 17 that it is up to the judge to authorise or order by order the seizure of e-mails or records of communications of a similar nature found in the course of computer searches or other legitimate access to a computer system that appear to be of great interest to the discovery of the truth or to evidence, and that the system for seizing correspondence provided for in articles 178 and 179 of the Code of Criminal Procedure applies.

VI. Article 179(3) of the CCP requires that the Criminal Investigating Judge, as the judge of freedoms, rights and guarantees, as well as the guarantor of fundamental rights, even at the enquiry phase, must first take cognisance, on first viewing, of the e-mail that has been seized, under penalty of the nullity provided for in Article 120(2)(d) of the CPP, which does not necessarily have to be complete.

VII. It is also the responsibility of the Criminal Investigation Judge to order or authorise the attachment to the case file of e-mails that appear to be relevant to the evidence, by means of a reasoned and appealable order.

VIII. After the opening and first viewing by Criminal Investigation Judge and the exclusion of those that may conflict with the privacy of the person and have no relevance to the evidence, the Criminal Investigation Judge authorises the Public Prosecutor's Office, as the body responsible for directing the enquiry and investigation, and by virtue of the accusatory principle laid down in Article 32(5) of the Constitution of the Portuguese Republic, to select the e-mails that seem relevant to the discovery of the truth and to the evidence, and to present them to the Criminal Investigation Judge in order to order them to be added to the case file.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRL:2024:85.18.3TELSB.F.L1.9.76/

PORTO COURT OF APPEAL

- **Judgement of the Porto Court of Appeal, of 21-02-2024**

  Process no. 6415/23.9JAPRT-A.P1

  Rapporteur: High Court judge Paula Guerreiro

When it comes to locating the mobile phone of a possible victim of a homicide or other crime that has made it impossible for them to communicate, access can be had to the data held by communications service providers, which is still provided for in articles 187 to 189 of the CCP, which the Constitutional Court has ruled are not unconstitutional, and nothing prevents the authorities from accessing them when values such as security, democratic legality and the exercise of criminal prosecution in the fight against crime are at stake.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2024:6415.23.9JAPRT.A.P1.E2/

- **Judgement of the Porto Court of Appeal, of 28-02-2024**

  Process no. 79/19.1T9AMR.P1

  Rapporteur: High Court judge Maria Deolinda Dionísio

I – The Constitutional Court Judgement no. 268/22, of 19 April, declares the unconstitutionality, with general binding force, of the rule contained in Article 4 of Law no. 32/2008, of 17 July, in conjunction with Article 6 of the same law, as well as the rule in Article 9 thereof, regarding the transmission of stored data to the competent authorities for the purpose of investigating, detecting and prosecuting serious crimes, insofar as it does not provide for notification to the person concerned that the stored data has been accessed by the criminal investigation authorities, from the moment that such communication is not likely to jeopardise investigations or the life or physical integrity of third parties.

II - Articles 187 to 189 of the Code of Criminal Procedure regulate the use of data relating to telephone conversations or communications in real time, while access to data held by operators for past telephone conversations or communications is regulated by law no. 32/2008 of 17 July.

III - The doctrine speaks of a trilogy of sources of digital evidence, namely the Code of Criminal Procedure, in articles 187 to 190, Law 32/2008 of 17/07, the so-called metadata law, and Law 109/2009 of 15/09, the Cybercrime Law, three pieces of legislation to regulate partial aspects of the same concrete reality.

IV - The indication of a mobile phone number by an operator is not void if the information was requested under the terms of articles 187 to 189 of the Code of Criminal Procedure, with the authorisation of the holder of the mobile phone to which the call was made, within a month of the date of the facts, and was communicated to the defendant when the charges were brought.

IV - But even if it were considered that the information had been provided within the scope of the metadata law, this would only mean that it could not be considered as evidence and not that the indictment would be null and void, and it would still be upheld on the basis of the other existing evidence.

V - With regard to prohibited evidence, it is clear from the law that while evidence obtained through torture, coercion or offence against people's physical or moral integrity

cannot be granted or compressed, and is irremediably and inexorably null and void because it affects the essence of fundamental rights of a personal nature, the nullity of the other types, those relating to intrusion into private life, home, correspondence or telecommunications, can be remedied with the consent of the holder.

VI - The diversity of regimes is based on the different nature and essence of the values in need of protection, and it was understood that the latter could remain at the free disposal of the respective holder as they did not attack the fundamental core of personality rights.

VII - However, although this system of absolute and relative nullities is similar to the legal provisions of articles 118 and 119 of the Code of Criminal Procedure, their scope and system do not coincide, since the latter are not remediable by the passage of time, but rather by the consent of the holder, which may be prior, subsequent or evidenced by express acts of renunciation of the invocation of the nullity committed by undue intrusion into rights of a personal nature, with legal and constitutional guarantees, such as the reservation of private life.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2024:112.20.4GAETR.P1.12/

- **Judgement of the Porto Court of Appeal, of 04-03-2024**
  Process no. 8233/21.0T8VNG-A.P1
  Rapporteur: High Court judge Teresa Sá Lopes

I - What is decided in the precautionary procedure in terms of the merits does not have repercussions on the merits of the action, just as the conviction formed in the precautionary procedure, based on a piece of evidence, on a certain matter of fact, is also not binding, i.e. the judgement that may be formed in the action in this regard may be different.

II - A different issue is whether a decision made immediately in a precautionary procedure on the admissibility of a certain piece of evidence is valid for the main proceedings.

III – "The images captured by a video surveillance system should be accepted as evidence in disciplinary proceedings and in subsequent legal action in which the application of a disciplinary sanction is discussed, particularly dismissal, provided that the assumptions arising from the legislation on data protection are observed and that it is concomitantly

concluded that the purpose of their placement was not exclusively to monitor the employee's professional performance."

IV - This is the case within the circumstantial framework established by the fact that the B recording system...was installed in the work vehicle in order to be closer to the customers being transported and to calculate the weekly results, not with a view to monitoring the professional performance of the drivers.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2024:79.19.1T9AMR.P1.C5/

- **Judgement of the Porto Court of Appeal, of 24-04-2024**
  Process no. 914/21.4T9VFR.P1
  Rapporteur: High Court judge Raquel Lima

I - As the appeal concerns an investigative decision, there is no need to investigate the existence of the defects in Article 410(2) of the Code of Criminal Procedure, relating to the judgement.

II - In order to assess the appeal against the investigative decision, it is necessary to analyse all the evidence in the case, both that which was already in the investigation and that which was produced during the pre-trial phase.

III - If there is some evidence that an offence has been committed, but it is so tenuous that it would not support a conviction at trial, the decision should be not to indict.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2024:914.21.4T9VFR.P1.57

- **Judgement of the Porto Court of Appeal, of 03-06-2024**
  Process no. 3326/22.9T8VFR-A.P1
  Rapporteur: High Court judge Ana Paula Amorim

I - The Bank's refusal under the duty of banking secrecy is legitimate when it comes to attaching documents issued by third parties, who are not parties to the action and do not authorise disclosure of their identity, and which prove the movements in the bank account held by the plaintiff.

II - In weighing up the preponderant interest, the interest in the administration of justice prevails over the private interest, which justifies waiving banking secrecy for the defendant bank to attach documentary evidence of the origin (instructions) and destination (beneficiaries) of the bank transactions carried out on the current account held by the plaintiff and to authorise the employees named as witnesses to testify on this matter, with a view to proving the bank movements on the account held by the plaintiff and referred to in the petition and defence.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2024:3326.22.9T8VFR.A.P1.24/

- **Judgement of the Porto Court of Appeal, of 09-09-2024**
  Process no. 3958/21.2T8VNG.P1
  Rapporteur: High Court judge Eugénia Pedro

I - Article 22(1) of the Labour Code guarantees the right to privacy and confidentiality with regard to personal messages and access to information of a non-professional nature that the employee sends, receives or consults, namely via e-mail.
II - If the employer provides the employee with a professional e-mail account and does not prohibit its use for personal purposes by establishing rules for the use of, the employee cannot access the content of e-mails and their attachments sent or received in that account, even if they are not marked as personal or if it does not appear from their external data that they are personal.
III - During the term of the employment contract, the employee's obligation not to compete is a corollary of the duty of loyalty towards the employer.
IV - At the end of the employment contract, without a non-competition pact having been signed with the employer, the worker regains the constitutionally guaranteed freedom to work, subject only to the restrictions common to any other citizen, namely the prohibition of unfair competition.
V - Subordinate workers who work as accountants for a company, terminate their employment contracts and start working as accountants on their own account, attracting some of their ex-employer's clients, do not incur in unfair competition, and it is not proven that this occurred before the termination of their contracts, nor that they used any

dishonest means that could be considered unfair competition or that they used information reserved by their ex-employer.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2024:3958.21.2T8VNG.P1.C4/

- **Judgement of the Porto Court of Appeal, of 12-09-2024**

  Process no. 2276/23.6T8MAI.P1

  Rapporteur: High Court judge Judite Pires

  I - The provision of statements relating to identified bank accounts for a limited period of time does not in itself constitute a violation of privacy, in the constitutional sense of this right.

  II - The requirement to disclose elements of a party's bank account that allow the verification of bank movements necessary to clarify disputed matters alleged by the other party, within the scope of what is strictly indispensable for the realisation of the evidential purposes sought by that party, and with strict observance of the principle of the prohibition of excess, is a guarantee of the fair co-operation of the parties with the Court, with a view to discovering the truth, in the light of the doctrine of weighing up interests, otherwise the right of the interested party to demonstrate, by those means, the factuality alleged by him of the production of the evidence he has indicated and to achieve effective judicial protection will be insanely compromised.
  https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2024:2276.23.6T8MAI.P1.E4/

- **Judgement of the Porto Court of Appeal, of 16-10-2024**

  Process no. 2276/23.6T8MAI.P1

  Rapporteur: High Court judge António Luís Carvalhão

I - The collection of CCTV images in some companies/establishments (such as supermarkets, which are open to the public) may be objectively indispensable for reasons of the safety of people and property, and is not to be confused with the exercise of remote supervision.

II - The fact that the collection of images by a video surveillance system sometimes involves a certain amount of monitoring of the workers who work in these companies is a fact that cannot be eliminated and must be tolerated to the extent that, when analysing the different rights at stake, the interests of the employer and, sometimes, of the workers themselves, take precedence; this is what has been termed *pre-intentional* monitoring.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2024:2276.23.6T8MAI.P1.E4/

- **Judgement of the Porto Court of Appeal, of 16-10-2024**
  Process no. 112/20.4GAETR.P1
  Rapporteur: High Court judge Maria José Ferrera Lopes

I – The Law no. 58/2019, of 8/08, does not define the lawfulness or unlawfulness of the collection or use of images, and the existence or non-existence of a licence granted by the National Data Protection Commission (CNPD) for the placement of video surveillance cameras only constitutes non-compliance with data protection legislation.
III - Evidence obtained through video surveillance does not constitute prohibited evidence when the purpose of this mechanical system is to protect property from attempted theft and it is not placed in a private or partially restricted location, even if it is not licensed by the CNPD.
III - Capturing images of a possible suspect of an illegal act in a banking institution is a necessary and appropriate means of repelling illegal aggression, not only against the property of the offending banking institution, but also against all citizens who have deposited money there, and does not constitute prohibited means of proof under the terms of Article 126/3 of the Criminal Procedure Code and does not contravene any rule of fundamental law.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2024:112.20.4GAETR.P1.12/

- **Judgement of the Porto Court of Appeal, of 23-10-2024**
  Process no. 1049/18.2JAPRT.P1
  Rapporteur: High Court judge Lígia Figueiredo

I - Criminal proceedings have their own moments for hearing nullities or other prior or incidental issues, and it is in the preliminary phase of the trial when the case file is received, Article 311(1) of the CCP, that the judge rules on prior or incidental issues that hinder the merits of the case, and later, already in the introductory acts, he also rules on nullities or incidental issues that may hinder the assessment of the case, but only on which there has not yet been a decision.

II - The crime of embezzlement provided for in Article 20(2) of Law 34/87 of 16 July does not require the appropriation of the property, but it does require the acts of the owner. Whereas in the crime of embezzlement of use, provided for and punished in Article 21(1) of Law no. 34/87 of 16 July (...) "It is a temporary use (aimed at the replacement or restitution of things improperly used), (...) without *animus domini*".

III - Since the catalogue crime, a crime of embezzlement provided for and punishable by Article 20(2) of Law 34/87, under which the collection of images by the criminal police was authorised, has fallen, the images collected have no legal support, since the crime resulting from the proven factuality, the crime of embezzlement of use provided for and punishable by Article 21 of the same law, is not part of the catalogue crimes listed in Article 1 of Law 5/2002 of 11 January.

IV - Notwithstanding the contemporaneity between the surveillance carried out and the collection of images, we are dealing with procedural steps that are autonomous from each other, in which the invalidity of the collection of images does not affect the surveillance carried out, which naturally preceded them, and also the facts that the inspectors/witnesses saw and later reported in their respective testimonies at the hearing.

V - The surveillance carried out by the Judiciary's witness inspectors, under the delegation of competence from the Public Prosecutor's Office with a view to investigating an indicted public crime, on acts that, although belonging to private life, take place in a public space, without preserving them themselves, is legally covered by the provisions of Article 171 of the CCP and does not violate the right to privacy provided for in Article 80 of the Civil Code and enshrined in Article 26 of the Constitution of the Portuguese Republic.

VI - The actions of the beneficiary of the use permit in the crime of embezzlement provided for and punished in Article 21(1) of Law 34/87 of 16 July are not covered by the legal protection of the rule, and are a case of improper necessary participation.
VII - In the light of a teleological interpretation, Article 29 of Law 34/87 of 16 July cannot be interpreted in a way that is restricted to the time period in which the crime was committed, otherwise the legal provision would be rendered useless.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2024:1049.18.2JAPRT.P1.A7/

- **Judgement of the Porto Court of Appeal, of 07-11-2024**
  Process no. 1560/22.0T8OVR.P1
  Rapporteur: High Court judge Isabel Ferreira

I - The question of whether or not a document containing a particular person's health data can be valued as evidence is unofficial knowledge.
II - The fact that the insurer has obtained this document, analysed it in order to refuse payment of the insured capital on the basis of it, declaring “the claim”, and attaching it to the case file constitutes “data processing” for the purposes of applying the general data protection regime.
III - Since consent was given by the data subject autonomously from the contractual clauses, the declaration is detached from the rest of the contract, and in fact exists in two different places, at the end of the contractual proposal and in the document containing the health questionnaire, and the information necessary to understand what was at stake was provided, with the purposes of the data processing signalled, and the declaration of consent having been given in an unequivocal, explicit, free and specific manner, the attachment of the document containing health data is lawful and can be taken into account by the court when judging the facts.
IV - A simple discharge note, from the palliative care service, which contains vague and generic information about “personal history”, without clinical documentation attached, is not enough to prove that the insured suffered from certain pathologies and that she did not communicate this information to the insurer.

V - In fulfilling the duty of care with regard to the information duties incumbent on the policyholder, they must behave with the honesty typical of ordinary citizens, who do not have to emphasise anything unfavourable to them.

VI - If there is a health questionnaire and consent to access and process health data, this duty on the part of the policyholder must be analysed with greater temperance, taking into account the fact that the policyholder considers that any "forgetfulness" can be made up for by the access he or she gives to his or her health data, which obviously has implications for the analysis of his or her possible negligence or intentional omission of information.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2024:1560.22.0T8OVR.P1.1A/

- **Judgement of the Porto Court of Appeal, of 11-12-2024**

  Process no. 337/24.3PHMTS-A.P1

  Rapporteur: High Court judge Maria Deolinda Dionísio

I – The use of GPS data in criminal investigations to obtain the geographical location of a target in real time is an atypical method of obtaining evidence, permitted by Article 125 of the Code of Criminal Procedure and subject to the legal regime of cellular location, provided for in Article 187(1) and (4), by virtue of Article 189(2) of the aforementioned law, and therefore depends on the prior authorisation of the Criminal Investigation Judge.

II – Data stored in safety or driver assistance equipment for motor vehicles, e.g. GPS, ECall-SOS, Via Verde, etc., which exist and would continue to exist independently of any criminal investigation, thus escaping the provisions of the aforementioned Article 187, can be obtained by the respective holder, but their use and inclusion in criminal proceedings depends on prior validation by the Criminal Investigation Judge.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRP:2024:337.24.3PHMTS.A.P1.04/

COIMBRA COURT OF APPEAL

- **Judgement of the Coimbra Court of Appeal, of 05-03-2024**

  Process no. 1337/22.3T8LRA-A.C1

  Rapporteur: High Court judge Teresa Albuquerque

I - In a declaratory action concerning the collusion of a husband, wife and daughter in the removal from the latter's assets of a certain property so that it would not be covered by an imminent execution, given the defence of the daughter and the wife that they had made bank transfers corresponding respectively to the acts of purchase and sale and partition relating to that property, proof of which they attached to their respective defences, it should be considered admissible for the plaintiff to request from the banks involved in those operations not only statements confirming those transfers as to date, amount, origin and destination, but also statements from the mother's and daughter's accounts relating to a significant period of time so that they can be analysed to prove the origin of the amounts involved and their non-receipt, without the interest in protecting bank secrecy, the privacy of private life and data protection having to prevent the obtaining of these means of proof, because, in this situation, the interest of the administration of justice and the principle of effective judicial protection should override them.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRC:2024:1337.22.3T8LRA.A.C1.A6/

- **Judgement of the Coimbra Court of Appeal, of 15-03-2024**

  Process no. 2596/23.0T8VIS-B.C1

  Rapporteur: High Court judge Paula Maria Roberto

I - Expert evidence should only be rejected if it is impertinent or dilatory, and cannot be rejected on the grounds that the matter in question can be proved by other means.

II - The expertise directed at all the computer and technological equipment of a third-party company and in a generic way at downloads of information on its equipment, without further ado, violates commercial secrecy, and there is no legal basis for breaking it.

III - The personal data of the clients/patients of the third-party company is protected under the terms of the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016) and by Law no. 58/2019 of 18/08, which ensures the implementation of this regulation in the national legal order, so access to it can only take place under the terms of this legislation, with the consent of the respective holders.

IV - Such an expertise is not proportional, given that such evidence would violate the rights of third parties enshrined in Article 26(2) of the Constitution of the Portuguese Republic.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRC:2024:2596.23.0T8VIS.B.C1.EC/

- **Judgement of the Coimbra Court of Appeal, of 20-03-2024**

  Process no. 60/23.6JALRA-A.C1

  Rapporteur: High Court judge Helena Lamas

I. The obligation to undergo photographic and lophoscopic identification when a measure of deprivation of liberty is applied [art. 3(1)(a)-ii) of Law 67/2007] does not violate the constitutional principles of equality, necessity and proportionality, in conjunction with the rights to personality, dignity, privacy and the protection of the defendant's personal identity.

II. If the defendant refuses photographic and lophoscopic identification, the judge may authorise the use of physical force to the extent necessary to comply with that legal obligation.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRC:2024:60.23.6JALRA.A.C1.B7/

- **Judgement of the Coimbra Court of Appeal, of 21-05-2024**

  Process no. 5777/22.0T8CBR.C3

  Rapporteur: High Court judge Teresa Albuquerque

I - The presuppositions of the special procedure for the protection of personality, currently laid down in Articles 857 to 880 of the Code of Civil Procedure, are the existence of a

threat to the physical and moral personality of a natural person ("human being", which means that legal persons are excluded), and the requirement that this threat be unlawful and direct.

II - The fact that the Applicant, who was declared bankrupt more than twenty years ago, was rehabilitated under the then articles 238 and 239 of the CPEREF (*Code of Special Processes for Company Recovery and Bankruptcy*), because it was under the terms of point c) of that Article 238, and therefore remained a debtor of the Respondent Bank, does not give him the "right to forget" these debts, as happens to some extent in the CIRE (*Insolvency and Company Recovery Code*), due to the institute of exoneration of the remaining liabilities, especially since it is not excluded that the Applicant, although bankrupt, could not have filed for insolvency and benefited from this institute.

III - Under the terms of Article 17/3 of General Regulation (EU) 2016/679 of 27 April of the European Parliament and of the Council, the right to be forgotten does not prevail if, in weighing up the values it requires, it is concluded that prolonging the retention of the negative personal data in question is necessary for the fulfilment of a legal obligation or for the performance of a task carried out in the public interest.

IV - The Defendant bank, like the other banks, and as is clear from Article 3 of Decree-Law 204/2008 of 14 October, is obliged to provide the Bank of Portugal Liability Centre (CRC) with information on actual or potential liabilities arising from credit operations granted in Portugal, a duty which is of indisputable public interest.

V- Restrictions such as the refusal to open a bank account and the denial of credit to purchase goods or services, or the limitation on the choice of work to be carried out in accordance with the respective professional qualifications, conflict with a wide range of rights of a personal nature that can be categorised as rights, freedoms and guarantees, affecting not only civil capacity, but also good name and reputation and economic rights, linking them to the dignity of the human person and to individual freedom itself.

VI - However, it is not the above-mentioned conduct of the Defendant Bank that affects these rights, so we cannot speak of a direct threat, as is presupposed by the aforementioned Article 878.

VII - Therefore, there is no need to consider whether the aforementioned restrictions on civil capacity should be considered disproportionate and excessive in relation to the

purpose to be achieved by the Defendant's actions before the (*Criminal Record Certificate*) CRC.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRC:2024:5777.22.0T8CBR.C3.A3/

- **Judgement of the Coimbra Court of Appeal, of 11-12-2024**
  Process no. 698/21.6JGLSB.C1
  Rapporteur: High Court judge Maria José Guerra

I - In telecommunications, a distinction must be made between basic data (technical support and connection elements that are not related to the communication itself, namely those related to the identification of the holders of a particular mobile phone card or IP), traffic data (elements that refer to the communication but do not involve its content, for example, the location of the user of the mobile equipment, as well as the recipient, the date and time of the communication, its duration, frequency, etc.) and content data (elements that refer to the content of the communication itself).
II - The data identifying the IP holder is of a permanent nature, resulting from the contractual elements entered into by the customer with the telecommunications service provider, and has nothing to do with data relating to electronic communications as such.
III - Since this data does not relate to communications made, processed and stored under Law 32/2008 of 17 July, but to contractual elements of a permanent nature that can be obtained independently of any communication, its collection by the judicial authorities falls outside the scope of the law and the declaration of unconstitutionality made by the Constitutional Court's 268/2022 judgement.
IV - Even if it is understood that the retention of basic data (which includes the name and address of the subscriber or registered user to whom the IP protocol address is assigned) is related to Law no. 32/2008, of 17 July, nevertheless, "despite the declaration of unconstitutionality ... the judicial authorities would always be allowed to obtain the address of the holder of the contract corresponding to the IP used in the commission of the crime under investigation ..." because "the conservation and storage of basic data, namely IP subscriber data by service providers, has not been prohibited", as this data must be conserved, as determined by Article 4(1)(a), Part 2 and no. 2(b)(iii).

V - When investigating a crime of child pornography committed by means of a computer system and in relation to which it is necessary to collect evidence in electronic form, the judicial authority may, under Article 14 of Law no. 109/2009 of 15 September, request the service provider to identify the subscriber of the IP in order to prove the crime by the person concerned, as this law has not been declared unconstitutional.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRC:2024:698.21.6JGLSB.C1.C0/

ÉVORA COURT OF APPEAL

- **Judgement of the Évora Court of Appeal, of 10-02-2024**
  Process no. 2524/21.7T8PTM-F.E1
  Rapporteur: High Court judge Vítor Sequinho dos Santos

1 - If the holder of a document ordered to be produced by the court wishes to refuse to do so, or wishes to do so by concealing part of the content of the document, by invoking a just cause - bank secrecy, protection of personal data or other - he has the burden of doing so until the procedural moment provided for in Article 417(3) of the Code of Civil Procedure (CPC).
2 - Failure to do so excludes the possibility of the holder of the document refusing to produce the document, or of presenting it while concealing part of its content, by invoking the aforementioned just cause.
3 - If the holder of the document refuses to produce it at the procedural moment provided for in Article 417(3) of the CPC, on the grounds that it is subject to banking secrecy, and the court provided for in Article 135(3) of the Code of Criminal Procedure (CCP) decides to break the secrecy, the holder is prohibited from presenting the document by concealing part of its content, even if he claims to be doing so in compliance with the legal regime for the protection of personal data.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRE:2024:2524.21.7T8PTM.F.E1.90/

- **Judgement of the Évora Court of Appeal, of 05-03-2024**

  Process no. 355/22.6JGLSB.E1

  Rapporteur: High Court judge Fátima Bernardes

I - Despite the form used by the Public Prosecutor's Office (invoking Article 14 of Law no. 109/2009 and articles 267, 262 and 164 of the Code of Criminal Procedure as the legal basis for the request), if the data requested is obtained from a specific IP in connection with a certain communication made (and not from a contractual relationship), we are dealing with data kept by the operator under the terms of Article 4(1)(a) and (2)(b) of Law 32/2008 of 17 July (which was declared unconstitutional, with general binding force, by Constitutional Court judgement no. 268/2022).

II - It is therefore prohibited evidence, and the partial admission of the facts by the defendant should not, in the case in point, be considered as an autonomous and independent form of access to the facts, with no close connection to the prohibited evidence, insofar as it is motivated by the seizure and examination of computer equipment where material with criminal relevance is discovered (which is prohibited evidence contaminated by the original prohibited evidence).

III - By virtue of the "remote effect" of that prohibition of evidence (primary evidence), the seizure of the computer equipment/material, which took place within the scope of the house search carried out, is "contaminated" and the evidence obtained by that means (sequential or secondary evidence) cannot be used, and, in the specific case, there is no exception or limitation to the "remote effect" arising from the aforementioned prohibition of evidence, namely the existence of sequential evidence obtained through an independent and autonomous source of the evidence in question or the occurrence of the situation of "dissipated taint".

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRE:2024:355.22.6JGLSB.E1.6D/

- **Judgement of the Évora Court of Appeal, of 06-06-2024**

  Process no. 2500/23.5T8FAR.E1

  Rapporteur: High Court judge Manuel Bargado

I - The blood collection test report carried out on the appellant was drawn up by the Technical and Quality Manager of the Forensic Chemistry and Toxicology Service, Southern Delegation of the Institute of Forensic Medicine, who is competent for this purpose, and therefore qualifies as an authentic document (Articles 363(2) and 369(1) of the Civil Code).

II - Authentic documents are full proof of the facts they refer to as having been carried out by the respective authority or public official and this probative force can only be rebutted on the grounds of their falsity (articles 371(1) and 372(1) of the same Code).

III - The prohibition on processing personal data relating to health, provided for in Article 9(1) of the GDPR, does not apply when the case provided for in Article 9(2)(f) of the same provision is met: "[if] the processing is necessary for the establishment, exercise or defence of legal claims or where the courts are acting in their judicial capacity".

IV - This is the situation in the case at hand, in which the exercise of the plaintiff's right of recourse is at issue, and access to blood alcohol content (BAC) should always be considered to be included in the permission relating to the exercise of the judicial function.

V - Since it is not possible that, at the time of the accident, the appellant had a BAC lower than the 1.30g/l he recorded three hours and nine minutes after the accident, and which resulted from the blood test carried out, even though the exact value of the BAC the defendant had has not been ascertained, the rate of 1.30g/l should be considered.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRE:2024:2500.23.5T8FAR.E1.02/

- **Judgement of the Évora Court of Appeal, of 11-07-2024**

  Process no. 1692/23.8T8STB-A.E1

  Rapporteur: High Court judge Anabela Luna de Carvalho

1 - Data relating to the health of a deceased person is protected under the terms of the General Data Protection Regulation (GDPR) and the national implementing law (Law no. 58/2019 of 08 August) because it falls within the special categories of personal data;

2 - All data relating to the state of health of a data subject that reveals information about their physical or mental health should be considered personal data, which includes

information about the natural person collected while alive during the provision of health services by health centres or hospital institutions - see Recital 35 of the GDPR (interpretative source);

3 - This intrinsically personal data is categorised as "sensitive data" in Recital 51 of the GDPR;

4 - As such, their processing is prohibited under the terms of Article 9(1) of the GDPR;

5- This will not be the case if the data subject has given his or her explicit consent to the processing of such personal data for one or more specific purposes, or if the processing is necessary (principle of necessity) for the establishment, exercise or defence of legal claims, or where the courts are acting in their judicial capacity pursuant to Article 9(2) of the GDPR;

6 - Because the law does not distinguish, the purpose "defence of a right in legal proceedings" can cover either a right of the data subject or a right against the data subject.

7 - What must be taken into account is the actual need to process the data, which must be done in a proportionate manner, restricted to the purpose that justifies it.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRE:2024:1692.23.8T8STB.A.E1.28/

- **Judgement of the Évora Court of Appeal, of 26-09-2024**

  Process no. 1442/23.9T8STR.E1

  Rapporteur: High Court judge Mário Branco Coelho

1. With the General Data Protection Regulation (GDPR) and the national law that implements it - Law 58/2019 of 8 August - it is no longer necessary to request authorisation or make any notification to the National Data Protection Commission in order to install a video surveillance system in the workplace.

2. Article 5(2) of the GDPR enshrines the principle of responsibility - or self-responsibility - with the data controller having a duty to ensure compliance with the principles relating to the processing of personal data (lawfulness, loyalty and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality).

3. The CNPD (*National Data Protection Commission*) no longer has the power to authorise or license the installation of a remote surveillance system in the workplace, and it should be understood that Article 21(1) of the Labour Code is tacitly repealed by the aforementioned Article 5(2) of the GDPR.
4. Article 20(2) of the Labour Code, by allowing the use of means of remote surveillance in the workplace whenever the purpose is the protection and safety of people and property, encompasses within its scope the protection of the employer's property, whether against the acts of third parties or against the acts of the workers themselves.
5. Recorded images and other personal data recorded through the use of video systems or other technological means of remote surveillance may be used for the purposes of establishing disciplinary responsibility, to the extent that they are used in criminal proceedings.
6. In the case of a theft offence committed by the employer's employees, the employer can lawfully use the images obtained from the video surveillance system installed in its establishment for disciplinary purposes, without being obliged to wait for the criminal proceedings to be concluded.
7. All the more so since Article 329(2) of the Labour Code obliges the employer to initiate the disciplinary procedure within 60 days of becoming aware of the offence, under penalty of forfeiture.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRE:2024:1442.23.9T8STR.E1.BE/

GUIMARÃES COURT OF APPEAL

- **Judgement of the Guimarães Court of Appeal, of 18-01-2024**
  Process no. 743/23.0JAVRL-A.G1
  Rapporteur: High Court judge Jorge Santos

- In order to determine the value of the action, which is equivalent to the immediate economic benefit of the claim, the specific claim formulated must be taken into account and, as analysing the claim is not enough, the facts of the respective cause of action must be taken into account;

- It follows from the combination of articles 306 and 308 of the Code of Civil Procedure that, whatever the position of the parties regarding the value of the case, the judge must always set it, i.e. he is not exempt from doing so.
- And the determination of the value of the case is made on the basis of the elements of the case or, if these are insufficient, by means of the indispensable steps that the parties request or the judge orders.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRG:2024:1266.23.3T8BRG.G1.C8/

- **Judgement of the Guimarães Court of Appeal, of 23-01-2024**

  Process no. 743/23.0JAVRL-A.G1

  Rapporteur: High Court judge Isabel Cristina Gaio Ferreira de Castro

I- Detailed billing data and cellular location data that provide the geographical position of mobile equipment based on acts of communication, insofar as they are processed to enable the transmission of communications, are traffic data relating to telecommunications and are therefore covered by the constitutional protection afforded to the secrecy of telecommunications.

II- It has been the majority view that, in the case of "conserved" or "preserved" communications data, it is not possible to apply the provisions of Article 189 of the Code of Criminal Procedure - the extension of the wiretapping regime - to cases in which Laws 32/2008 and 109/2009 apply. In other words, for evidence of communications preserved or stored in computer systems, there is a new criminal procedural system, the one provided for in articles 11 to 19 of Law 109/2009, of 15 September, the Cybercrime Law, with the specificities mentioned above, assisted by articles 3 to 11 of Law 32/2008, if data is provided for in the latter.

The Constitutional Court's judgement no. 268/22, of 19 April, declared the unconstitutionality, with general binding force, of several provisions of Law no. 32/2008, specifically: the rule contained in Article 4 of Law no. 32/2008, of 17 July, in conjunction with Article 6 of the same law, for violation of the provisions of paragraphs 1 and 4 of Article 35 and paragraph 1 of Article 26, in conjunction with paragraph 2 of Article 18, all of the Constitution; and the norm of Article 9 of Law no. 32/2008, of 17 July, on the transmission of stored data to the competent authorities for the investigation, detection

and prosecution of serious crimes, insofar as it does not provide for notification to the person concerned that the stored data has been accessed by the criminal investigation authorities, from the moment that such communication is not likely to compromise the investigations or the life or physical integrity of third parties, in violation of the provisions of Article 35(1) and Article 20(1), in conjunction with Article 18(2), all of the Constitution.

III- At issue is the transmission by telecommunications service operators of stored traffic and cellular location data arising from the possession and/or use of telephone handsets, which, according to our understanding, is specifically regulated and governed by Law no. 32/2008.

However, the present case investigates facts that could be part of the commission of an arson offence, provided for and punishable by Article 274(1) of the Penal Code, with a prison sentence of 1 to 8 years.

This crime is not included in the catalogue of crimes that meet the definition of "serious crime" in Article 2(1)(g) of Law 32/2008, supplemented by the clarification in Article 1(i), (j) and (m) of the Penal Code as to what is meant by "terrorism", "violent crime" and "highly organised crime".

In fact, obtaining evidence of a stored cellular location can only be admitted when a *serious crime* is involved, according to the aforementioned narrow definition, which is an essential prerequisite for the application of Law 32/2008.

As such, the applicability of Law 32/2008 is inexorably ruled out and the assessment of the other assumptions on which it depends - namely the [procedural] quality of the person to whom the data whose transmission is sought refers, as required by Article 9(3) [namely, the suspect, provided for in point a)] - is prejudiced, as is the question of the effects arising from the declaration of unconstitutionality of some of its provisions in the aforementioned terms.

IV- Likewise, the applicability of the extension system provided for in articles 189(2) and 187 of the Code of Criminal Procedure should be ruled out, since the request is for past data to be kept, not future data or data in real time, a circumstance which, in itself, if we follow the understanding explained *above,* rules it out as unavoidable.

Even if this were not the case, despite the fact that this is a crime included in the catalogue of crimes listed in Article 187(1) [more specifically, in point a) - crimes punishable by a prison sentence of more than 3 years], the same is not true of the catalogue of the persons concerned listed in paragraph 4 of the same article, especially a person with the procedural status of *suspect* or *defendant* [point a)].

In fact, there aren't even any suspects in the enquiry. Article 1(e) of the Code of Criminal Procedure defines "suspect" as *"any person for whom there is evidence that he or she has committed or is preparing to commit an offence, or has participated or is preparing to participate in it"*. Now, as was asserted in the decision under appeal, the case law of the higher courts has widely held that if the cellular location data to be obtained does not target a suspect, but rather a universe of unidentified people united only by the simple fact of being in a given place at a given time, it is not admissible, since, in addition to not respecting the principles of proportionality and adequacy, it does not allow it to be included in the legal-penal concept of "suspect".

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRG:2024:743.23.0JAVRL.A.G1.2B/

- **Judgement of the Guimarães Court of Appeal, of 08-02-2024**
  Process no. 596/22.6T8VNF.G2
  Rapporteur: High Court judge Paulo Reis

I - The purpose of this action is to make effective the activation of the guarantees provided for in a group life insurance contract, whereby the defendant/insurer took on the coverage of the risk relating to the payment of the amount loaned to the plaintiff and her deceased husband, obliging itself to make this payment in the event of the random event provided for in the contract - in this case, the death of the insured person.

II - With the occurrence of the claim during the term of the insurance contract, in this case the death of the insured person, as a risk event triggering the right and a condition for its enforceability, all the constitutive requirements and conditions for the enforceability of the obligation to pay the sum insured are met.

III - It is duly established in these proceedings that the plaintiff/appellant subscribed, on 6-07-2020, to a claim report concerning the death of her husband, who was also insured,

to which she attached a medico-legal autopsy report containing the possible causes of the claim and its consequences, under the terms set out above, this is enough to consider that the appellant/insured has fulfilled the burden of reporting the claim and the duty to provide additional information about it, to the extent that it was required to do so, under the terms and for the purposes set out in the aforementioned Article 100(2) of the RJCS (*Legal Regime of the Insurance Contracts*).

IV - Health information is the property of the individual, and the circulation of health information must be ensured with respect for the security and protection of personal data and health information, so only the individual himself could dispose of it, and his will cannot even be replaced by the will of those who succeed him in his property rights.

V - Since the insurer had specific and autonomous written authorisation from the deceased insured to obtain the information it wanted, it could itself obtain the information it deemed necessary to ensure that it had to fulfil the agreed benefit in the event of the random event provided for in the insurance contract.

VI - Therefore, the insurer cannot seek to take advantage of the alleged need for more information to assess the claim, specifically on the date of diagnosis of certain pathologies suffered by the deceased insured, imposing on the appellant, who is also an insured party in the contract in question, to send a report from the deceased insured's treating doctor, indicating the date of diagnosis of the pathologies mentioned in the autopsy report (diabetes, hypertension and smoking) - letter dated 05-08-2020 - and, later, to send a report indicating the date of diagnosis of the following pathologies: type II diabetes mellitus and chronic liver disease (letter dated ..../.../2020), as these are elements that relate to the insured's personal health data, which the defendant has not demonstrated, nor claimed, to be available to the insured, the plaintiff, nor are they expressly or specifically provided for as a requirement for the settlement of the sums insured in the corresponding clause of the general conditions of the aforementioned policy.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRG:2024:596.22.6T8VNF.G2.81/

- **Judgement of the Guimarães Court of Appeal, of 19-03-2024**
  Process no. 204/23.8GBCHV-A.G1

Rapporteur: High Court judge Fátima Furtado

I- Law 32/2008 transposed into Portuguese law Directive 2006/24/EC of the European Parliament and of the Council of 15 March on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. With its entry into force, the procedural regime for telephone communications laid down in articles 187 to 190 of the Code of Criminal Procedure is no longer applicable to the collection of evidence by "preserved cellular location", which refers to the location of communications relating to the past, i.e. archived, which is one of the forms of electronic evidence collection.

II- A situation that remained, since in the Cybercrime Law, which comes after it, the legislator made a point of expressly proclaiming (in Article 11(2)) that the regime of Law no. 32/2008, of 17 July, would not be affected.

III- Law 32/2008 has been removed by virtue of the declaration of unconstitutionality, with general binding force, of the rule contained in Article 4, in conjunction with Article 6, on the grounds that they allowed disproportionate damage to the privacy of citizens (Constitutional Court Judgement no. 268/2022), the combined provisions of articles 189,(2) and 167 of the Code of Criminal Procedure, Article 6 of Law no. 41/2004 of 18 August (specifically Article 6(7)) and Article 14(3) of Law no. 109/2009 of 15 September cannot be reprised and applied instead, as the appellant argues.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRG:2024:204.23.8GBCHV.A.G1.A4/

- **Judgement of the Guimarães Court of Appeal, of 26-06-2024**

  Process no. 1303/19.6T8BRG.G2

  Rapporteur: High Court judge Paulo Reis

I - The law requires a special form for the validity of contracts concluded by telephone contact, making the consumer's acceptance of the contract subject to the written form, with the exception of cases in which the first telephone contact between the parties was made by the consumer.

II - Since the contract in question was concluded at a distance using the telephone and it is clear that the initial impulse was given by the supplier, the contract resulting from such

contact would only be valid and effective if the consumer signed the offer or sent his written consent to the service provider, which in this case did not happen, and therefore the contract is null and void due to non-compliance with the legally prescribed form.

III - In view of the nullity of the contract, the data controller lacks a legitimate interest in transmitting the plaintiff's data to the subcontractors, so that they could be included in the database shared by the companies offering electronic communications networks and services, and also in attempting to collect the amounts charged out of court.

IV - Since it has not been proven that the subcontractors' specific obligations have been violated, nor has it been alleged that they have not complied with the lawful instructions of the controller, it is not possible to make use of the civil liability mechanism provided for in Article 82/2 of the GDPR with regard to the former.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRG:2024:1303.19.6T8BRG.G2.58/

- **Judgement of the Guimarães Court of Appeal, of 27-06-2024**
  Process no. 5232/19.5T8VNF-H.G1
  Rapporteur: High Court judge Gonçalo Oliveira Magalhães

I - The nullity of a legal transaction on the grounds of contravention of the law presupposes the existence of a legal rule that directly or indirectly prohibits its conclusion.

II - This is the case with the rule in Article 6/1 of the CSC (*Commercial Companies Code*), which prohibits the conclusion of transactions that are neither necessary nor convenient for the pursuit of the purpose of commercial companies, which consists of obtaining profits to be shared by its shareholders or attributed to the sole shareholder, in the case of single-member companies.

III - The purpose should not be confused with the object of the company, which consists of the activity or set of activities that the company proposes to carry out in order to achieve that object.

IV - The assignment of credits that have their source in legal transactions of a banking nature, involving only the transfer of the active side of the obligatory relationship, is not, in itself, an act of a banking nature nor does it imply, for the assignee, the exercise of any activity exclusive to credit institutions and financial companies.

V - Therefore, the assignment of bank credits to a company that is neither a credit institution nor a financial company is not prohibited by Article 8 of the General Regime for Credit Institutions and Financial Companies, approved by Decree-Law no. 298/92, of 31 December.

VI - The assignment of bank loans is not prohibited either by Article 78 of the General Regime for Credit Institutions and Financial Companies or by Article 6/1 of 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, which are merely rules of conduct.

VII - Violation of these rules by the assignor, through (i) the communication to the assignee of information covered by secrecy that is not strictly necessary for the collection of the credit or (ii) the transmission of the assignee's personal data without observing the precautions required by law, may give rise to civil, criminal or administrative liability, but does not determine the nullity of the legal transaction resulting in the assignment of credits.

VIII - This understanding allows a balance to be struck between the assignor's right to credit and the rights of the assignee that are protected by the aforementioned rules, so that the rule that is thus drawn from them by way of interpretation does not affront the assignee's right to privacy and family life, enshrined in art. 26/1 and 2 of the Constitution of the Republic.

https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRG:2024:5232.19.5T8VNF.H.G1.E3/

- **Judgement of the Guimarães Court of Appeal, of 24-09-2024**

  Process no. 596/22.6T8VNF.G2

  Rapporteur: High Court judge Isilda Pinho

I. For the criminal offences set out in articles 383 and 382 of the Penal Code to be met, it is not enough for the official to abuse his functions or breach his duties in order to conclude that the offences in question are included, but it is also necessary for the agent to act with specific intent, with the intent determined in the legal precepts in question.

II. In other words, they require a special subjective element, which presupposes the verification of certain facts: the intention to obtain, for oneself or for another person, an illegitimate benefit or to cause harm to the public interest or to third parties [the offence of breach of secrecy by an official], the intention to obtain, for oneself or for a third party, an illegitimate benefit or to cause harm to another person [the offence of abuse of power].
III. When this fact does not appear in the indictment, a decision not to indict must be made.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRG:2024:178.19.0T9EPS.D.G1.98/

- **Judgement of the Guimarães Court of Appeal, of 24-10-2024**
  Process no. 4844/23.7T8BRG-A.G1
  Rapporteur: High Court judge António Beça Pereira

When it is necessary to break banking secrecy in order to discover the truth of the matter, in principle the interests protected by banking secrecy must give way to those underlying the realisation of justice.
But the principle of proportionality must be observed in the judgement.
https://jurisprudencia.csm.org.pt/ecli/ECLI:PT:TRG:2024:4844.23.7T8BRG.A.G1.67/