FIVELEX
STUDIO LEGALE E TRIBUTARIO

Regulatory update

Data protection, IP, IT e AI

n. 1 / 2024

DATA PROTECTION

30 April 2024 - Judgment of the EU Court of Justice in Case C-178/22: Privacy and prosecution of serious offences: the court responsible for authorising access to telephone records to identify the perpetrators of an offence, and for the prosecution of which offence national law envisages such access, must be entitled to refuse or restrict that access.

Under Italian law, the offence of aggravated theft is one of the offences that may justify obtaining telephone records from a provider of electronic communications services based on prior authorisation from a court. The Court of Justice considers that access to such records can be granted only to the data of individuals suspected of being implicated in a serious offence, and it specifies that it is for the Member States to define “serious offences”. However, the court responsible for authorising that access must be entitled to refuse or restrict that access where it finds that the interference with the fundamental rights to private life and to the protection of personal data which such access would constitute is serious, while it is clear that the offence at issue is not a serious offence in the light of the societal conditions prevailing in the Member State concerned.

---

30 April 2024 - Judgment of the EU Court of Justice in Case C-470/21 - Combating criminal offences and interference with fundamental rights: a national public authority responsible for combating online counterfeiting may access identification data on the basis of an IP address-

Member States may impose on internet access providers an obligation to retain IP addresses, in a general and indiscriminate manner, for the purposes of combating criminal offences in general, provided that such retention does not allow precise conclusions to be drawn about the private life of the person concerned. That can be achieved by retention arrangements that ensure a genuinely watertight separation of IP addresses and other categories of personal data, in particular civil identity data.

Member States may also, under certain conditions, authorise the competent national authority to access the civil identity data associated with IP addresses, provided that such retention – guaranteeing a watertight separation of the different categories of retained data – has been ensured.Where, in atypical situations, the specific features of a national procedure governing such access may – through the linking of the data and information collected – allow precise conclusions to be drawn about the private life of the person concerned, access must be subject to prior review by a court or by an independent administrative body.

FIVELEX
Studio Legale e Tributario
Via degli Omenoni 2
20121 Milano

Piazzale delle Belle Arti 6
0196 Roma

26 April 2024 - EU Regulation establishing the European Health Data Space (EHDS Regulation) definitively approved.

In its last legislative session, the European Parliament gave final approval - 445 votes to 142 - to the EU Regulation establishing the European Health Data Space (EHDS), implementing the agreement reached with the EU Council.

The European Health Data Space will be a key pillar of the European Health Union and is the first common EU data space in a specific area to emerge from the European Data Strategy. In essence, it is the first *lex specialis* with respect to the Data Governance Act (Regulation 2022/868 - DGA) which, as a *lex generalis*, sets the rules on the cross-sectoral circulation of data in European Data Spaces.

The EHDS will enable citizen-patients to take full control of their health data, facilitating their exchange for the provision of healthcare across the EU (so-called primary use of data circulating through a dedicated European electronic platform). A true single market for electronic health record systems is also promoted. Furthermore, a coherent, reliable and efficient system for the re-use of health data for research, innovation, development of personalised medicine and apps, training of AI algorithms, policy-making and regulatory activities is implemented: the so-called secondary use of data, for which a second and dedicated electronic platform will be activated.

At this point, it can be said that this EU Legislature that is coming to an end has been among the most relevant in terms of the full implementation of the EU regulatory framework implementing the Data Strategy: after the GDPR, the DGA, the Data Act and the EDHS, together with the cybersecurity framework (NIS 2, DORA, Critical Systems Resilience Directive, GPSR, CRA, TERREG).

---

22 April 2024 - Available from 22 April to 30 June 2024, the service to object to the automatic feeding of the Electronic Health Record by uploading health data prior to 19 May 2020.

In order to increase the feeding of the Electronic Health Record (Fascicolo Sanitario Elettronico - FSE), Article 11 of Decree-Law No. 34/2020 provided that, as of the date of publication of the decree (19 May 2020), the loading of data onto the FSE will take place automatically, with the consequent elimination of the 'consent to feeding' required by previous legislation.

For health data and documents generated by clinical events prior to 19 May 2020, the patient may exercise the right to oppose the feeding of the ESF through the online service 'ESF - Opposition to the past', which allows the patient to oppose the loading of digital health data and documents generated by clinical events referring to services provided by the National Health Service prior to 19 May 2020 into his or her ESF. Opposition to the uploading of data and documents generated by clinical events relating to services provided by the National Health Service prior to 19 May 2020 must be made through the Sistema Tessera Sanitaria portal at www.sistemats.it.

The online service "FSE - Opposition to the past" is available from 22 April until 30 June 2024.

The choice can be revoked and re-registered in the Sistema Tessera Sanitaria several times, until 30 June 2024. The system will select the last indication loaded chronologically.

Failure to access the online service "FSE - Opposition to the past" or accessing the service without registering one's opposition will result in the automatic upload of one's data and available health documents prior to 19 May 2020 into the FSE.

FIVELEX
Studio Legale e Tributario

Via degli Omenoni 2
20121 Milano

Piazzale delle Belle Arti 6
0196 Roma

23 April 2023 - Constitutional Court: Regions cannot autonomously regulate the processing of personal data.

A regional regulation governing the processing of personal data in the installation of video-surveillance systems is unconstitutional on the grounds that it infringes the obligations arising from Italy's membership of the European Union and encroaches on the State's exclusive legislative powers in the field of 'civil order'. This is what is stated in sentence no. 69/2024 by which the Constitutional Court declared article 3 of Apulia Region law no. 13 of 2023 to be constitutionally illegitimate due to its conflict with article 117, first and second paragraphs of the Constitution. The Court noted that the European Union, in the exercise of the competence set out in Article 16 of the Treaty on the Functioning of the European Union, lays down complex rules on the processing of personal data, which *'are completed and supplemented by national sources'*. According to the Court, the Region cannot regulate the matter autonomously, nor can it make a selection of sources and provisions, "*which, within the complex set of rules contemplated both by the European Union and by the State legislature, are called upon to regulate this complex and delicate matter*", because in so doing it *'not only overlaps with the European Union and State legislation, exceeding its own competences, but moreover makes an arbitrary choice, whose prescriptive content is tantamount to considering binding only the rules identified by the regional legislature and not also the others'*, dictated by the European Union and the State legislature.

18 April 2024 - EDPB sets out priorities for 2024-2027 and clarifies implementation DPF redress mechanisms.

During its latest plenary, the EDPB adopted its strategy for 2024-2027. The strategy sets out the EDPB's priorities, grouped around four pillars, as well as key actions per pillar to help achieve these objectives. These four pillars are:

Pillar 1 – Enhancing harmonisation and promoting compliance

Pillar 2 – Reinforcing a common enforcement culture and effective cooperation

Pillar 3 – Safeguarding data protection in the developing digital and cross-regulatory landscape

Pillar 4 – Contributing to the global dialogue on data protection

In the next four years, the EDPB will continue to promote compliance with data protection law by developing clear, concise and practical guidance on important topics, and by developing materials for a wider audience. In addition, enforcement cooperation will remain an important priority for the EDPB. The Board will continue building on the vision set out in its so-called Vienna Statement, and further develop EDPB initiatives in this area, such as the coordinated enforcement actions.

A new aspect of the strategy is the focus on the interplay with the new regulatory digital framework. New digital laws, such as the DMA or the DSA, have an impact on data protection and privacy. The EDPB will work to enhance cooperation with other regulatory authorities, with a view to embedding the right to data protection in the overall regulatory architecture. Furthermore, the EDPB will continue to pay special attention to challenges raised by new technologies, such as AI.

The strategy will be complemented by two work programmes, which will contain details about its implementation.

In addition, regarding the EU-US Data Privacy Framework (DPF), the EDPB adopted Rules of Procedure, a public information note and template complaint forms to facilitate the implementation of the redress mechanisms under the DPF.

The EDPB documents relate to two DPF redress mechanisms created to handle complaints by EU individuals. The redress mechanisms deal only with complaints concerning their respective competence - national security or commercial purposes - and only for data transmitted after 10 July 2023.

---

17 April 2024 – European Data Protection Board (EDPB) - Opinion 8/2024 on the on line "*Pay or Consent*" mechanism.

During its latest plenary, the EDPB adopted an Opinion following an Art. 64(2) GDPR request by the Dutch, Norwegian & Hamburg Data Protection Authorities (DPA). The Opinion addresses the validity of consent to process personal data for the purposes of behavioural advertising in the context of consent or pay' models deployed by large online platforms.

As regards 'consent or pay' models implemented by large online platforms, the EDPB considers that, in most cases, it will not be possible for them to comply with the requirements for valid consent, if they confront users only with a choice between consenting to processing of personal data for behavioural advertising purposes and paying a fee.

The EDPB considers that offering only a paid alternative to services which involve the processing of personal data for behavioural advertising purposes should not be the default way forward for controllers. When developing alternatives, large online platforms should consider providing individuals with an 'equivalent alternative' that does not entail the payment of a fee. If controllers do opt to charge a fee for access to the 'equivalent alternative', they should give significant consideration to offering an additional alternative. This free alternative should be without behavioural advertising, e.g. with a form of advertising involving the processing of less or no personal data. This is a particularly important factor in the assessment of valid consent under the GDPR.

The EDPB stresses that obtaining consent does not absolve the controller from adhering to all the principles outlined in Art. 5 GDPR, such as purpose limitation, data minimisation and fairness. In addition, large online platforms should also consider compliance with the principles of necessity and proportionality, and they are responsible for demonstrating that their processing is generally in line with the GDPR.

As regards the need for consent to be free, the following criteria should be taken into account: conditionality, detriment, imbalance of power and granularity. For instance, the EDPB points out that any fee charged cannot make individuals feel compelled to consent. Controllers should assess, on a case-by-case basis, both whether a fee is appropriate at all and what amount is appropriate in the given circumstances. Large online platforms should also consider whether the decision not to consent may lead the individual to suffer negative consequences, such as exclusion from a prominent service, lack of access to professional networks, or risk of losing content or connections. The EDPB notes that negative consequences are likely to occur when large online platforms use a 'consent or pay' model to obtain consent for the processing.

Controllers also need to evaluate, on a case-by-case basis, whether there is an imbalance of power between the individual and the controller. The factors to be assessed include the position of the large online platforms in the market, the extent to which the individual relies on the service and the main audience of the service.

Furthermore, the EDPB provides elements to assess the criteria of informed, specific and unambiguous consent that large online platforms should take into account when implementing 'consent or pay' models.

In addition to this Art. 64(2) Opinion, the EDPB will also develop guidelines on 'consent or pay' models with a broader scope and will engage with stakeholders on these upcoming guidelines.

11 April 2024 - Judgment of the Court of Justice of the EU in Case C-741/21 - Liability of the data controller for damage caused to third parties by its employee in breach of the data protection instructions received.

The EU Court of Justice provided the correct interpretations of Articles 82, 83 and 29 of the GDPR in the case of a German lawyer who had complained to a company about the continued receipt of unsolicited communications for marketing purposes even after his consent had been withdrawn.

The data subject therefore filed a lawsuit against the company for damages for the processing of personal data in which the company claimed that the breach was attributable to an employee who had infringed the strict protection system implemented by the company to avoid unsolicited calls and the instructions on processing given under Article 29 of the GDPR. When asked by the German national court about the interpretation of Article 82 of the GDPR regarding the exemption of the controller from liability, the CJEU on this point replied that Article 82 of the GDPR must be interpreted as meaning that it is not sufficient for the controller, in order to be exempted from liability under paragraph 3 of that article, to claim that the damage in question was caused by the failure of a person acting under his or her authority, within the meaning of Article 29 of that regulation. If that were the case, the damaged party would have to take direct action against the infringer, depriving him of his right to compensation for the damage. The Court points out that the circumstances of the exemption from liability provided for in Article 82(3) of the GDPR must be strictly limited to those in which the data controller is able to prove, on its part, that the damage was not attributable. Therefore, in the case of a personal data breach committed by a person acting under its authority, that controller may only benefit from this exemption if it proves that there is no causal link between the possible breach of the data protection obligation and the damage suffered by the data subject (in other words: the breach by the employee must be in pursuit of his own purposes and unconnected with the tasks and instructions to which he is subject).

The EU Court also sets out further important principles on the subject of compensation for damage caused by treatment, including the following: (1) an infringement of provisions of the GDPR which confer rights on the data subject is not sufficient, in itself, to constitute 'non-material damage' within the meaning of section 82 GDPR, irrespective of the degree of seriousness of the damage suffered by that person and the proof thereof; (2) must be interpreted as meaning that in order to determine the amount of damages due as compensation for damage based on that provision, it is not necessary, first, to apply *mutatis mutandis* the criteria for setting the amount of administrative fines laid down in Article 83 of that regulation and, second, to take account of the fact that several infringements of that regulation concerning the same processing operation affect the person seeking compensation.

7 Aprile 2024 – US House of Representatives released a draft of a bipartisan, bicameral federal privacy bill (the American Privacy Rights Act, or "APRA").

On April 7, US House of Representatives member Cathy McMorris Rodgers (R-WA) and Senator Maria Cantwell (D-WA) released a draft of a bipartisan, bicameral federal privacy bill (the American Privacy Rights Act, or "APRA"), aimed at putting people in control of their own personal data and eliminating the patchwork of state laws by setting one national privacy standard. If adopted, the APRA would have broad pre-emptive effect over many provisions of state-level data privacy laws.

Proposed American Privacy Rights Act of 2024 seeks to establish national consumer data privacy rights, govern Artificial Intelligence and automated decision-making, impose additional obligations on high-impact social media companies and large data holders, supersede state privacy laws, and allow private right of action.

The APRA applies to businesses subject to the authority of the Federal Trade Commission ("FTC"), common carriers, and nonprofits (together, "Covered Entities"), along with businesses that process covered data on behalf of or at the direction of Covered Entities ("Service Providers"). The APRA would impose obligations on Covered Entities and Service Providers to minimize processing of covered data and apply reasonable data security measures. The APRA also seeks to impose heightened obligations on high-impact social media companies and large data holders.

Additionally, the APRA seeks to create uniform data privacy rights for all persons residing in the US. These rights include the rights to opt out of targeted advertising and to view, correct, export or delete their data. In trend with Europe's data protection laws (the General Data Protection Regulation ("GDPR") and Digital Services Act ("DSA")) and some state privacy laws (e.g., the California Consumer Privacy Act ("CCPA")), the APRA also requires Covered Entities and Service Providers to provide increased transparency by mandating the inclusion of specific information on data processing, retention, transfers to third parties, security practices, and consumers' rights in their public facing privacy policies.

ARTIFICIAL INTELLIGENCE

24 Aprile 2024 - Council of Ministers: Bill approved for the introduction of provisions and the delegation to the Government in the field of Artificial Intelligence.

The Council of Ministers has approved, with the provision of the request to the Houses of Parliament for prompt scheduling in compliance with the regulations of the two branches of Parliament, a bill for the introduction of provisions and the delegation of powers to the Government on artificial intelligence.

The bill introduces rules of principle and sector provisions that, in the view of the Italian Government, do not overlap with the European Regulation on Artificial Intelligence (AI Act) approved last March 13 by the European Parliament, soon to be issued, but accompany its regulatory framework in sectors of domestic law. In fact, the bill aims to regulate the AI in five areas: national strategy, national authorities, promotional actions, copyright protection, and criminal sanctions. There is also a delegation of powers to the Government to adapt the national system to the EU Regulation in matters such as citizens' AI literacy (both in school and university courses) and training by professional bodies for professionals and operators. The delegation also concerns the reorganisation of criminal law to adapt offences and penalties to the unlawful use of AI systems.

19th April 2024 – Council of Europe (CoE) Parliamentary Assembly issues opinion on draft AI convention.

The Parliamentary Assembly of the Council of Europe (CoE) published its Opinion 303 (2024) on the draft *Framework on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law by the Committee on Artificial Intelligence*.

The Assembly must provide its opinion on the draft framework before it is adopted by the Committee of Ministers, after which it may be signed and ratified.

In particular, the Assembly provided that CoE Member States, when ratifying the draft framework, should opt to fully apply its provisions to the activities of private actors. Specifically, the Assembly provided that the draft framework does not address the risks and impacts arising from the use of artificial intelligence (AI) by private actors and that a differentiated approach for the private sector creates a significant loophole.

In addition, the Assembly proposed amendments to provisions on national security, proposing that AI activities necessary to protect national security only be possible if the activities are in line with international human rights law. The Assembly also proposed that Member States should establish mechanisms to ban or limit certain uses of AI systems where such use cases are considered incompatible with the respect of human rights, the functioning of democracy, and the rule of law.

Further proposals by the Assembly include the addition of appropriate measures to ensure the protection of whistleblowers in relation to activities within the AI lifecycle systems.

INFORMATION TECHNOLOGY

24 April 2024 – EU Parliament adopts the Electronic Platform Work Directive (the GIG Economy Directive).

The European Parliament definitively approved the new rules aiming to improve the working conditions of electronic platforms' workers. The new rules, agreed on by the EU Parliament and the EU Council in February and adopted with 554 votes in favour, 56 votes against and 24 abstentions, aim to ensure that electronic platforms' workers have their employment status classified correctly and to correct bogus self-employment. They also regulate, for the first time ever in the EU, the use of algorithms in the workplace.

The new law introduces a presumption of an employment relationship (as opposed to self-employment) that is triggered when facts indicating control and direction are present, according to national law and collective agreements, and taking into account EU case law.

The directive obliges EU countries to establish a rebuttable legal presumption of employment at national level, aiming to correct the imbalance of power between the digital labour platform and the person performing platform work. The burden of proof lies with the platform, meaning that it is up to the platform to prove that there is no employment relationship.

New rules on algorithmic management are also provided. The new rules ensure that a person performing platform work cannot be fired or dismissed based on a decision taken by an algorithm or an automated decision-making system. Instead, digital labour platforms must ensure human oversight on important decisions that directly affect the persons performing platform work.

Transparency and data protection rights are further enforced. The directive introduces rules that protect platform workers' data more robustly. Digital labour platforms will be forbidden from processing certain types of personal data, such as data on someone's emotional or psychological state and personal beliefs.

The agreed text will now have to be formally adopted by the Council, too. After its publication in the Official Journal of the EU, member states will have two years to incorporate the provisions of the directive into their national legislation.

20 April 2024 - Digital signature: disabled voters denied the possibility of signing electoral lists with digital signatures: issue referred to the Constitutional Court.

The Court of Civitavecchia raises a question of constitutional legitimacy concerning the preclusion, for persons with disabilities unable to sign, of signing a list of candidates for submission to the regional elections pursuant to Article 9 of Law no. 108/1968 with a digital signature.

An Italian citizen with a disability wished to exercise his right to sign the electoral lists for the election of the Regional Council, pursuant to Article 9 of Law no. 108 of 17 February 1968. He was unable to provide a handwritten signature due to his health condition and had provided himself with a digital signature that he could use independently.

The political group to which he applied represented to him that Article 9 of Law No. 108/1968, according to the interpretation adopted by the competent electoral offices, precluded the possibility of affixing signatures in digital format and that this preclusion also derived from Article 2(6) of Legislative Decree No. 82 of 7 March 2005 (Digital Administration Code).

The citizen therefore applied to the Region of Lazio, formally inviting it to expressly declare the possibility of affixing the signature provided for by Article 9, Law No. 108/1968 with a digital signature.
The request submitted by the citizen remained unanswered, while the same request - submitted by an association - was confirmed by the Region that it was impossible to collect the signature by digital signature.

The citizen therefore applied to the Court of Civitavecchia asking it to "ascertain and declare the applicant's right to sign a list of candidates for submission to the regional elections, pursuant to Article 9, Law no. 108/1968, with his own digital signature" and, in the alternative, "uphold the above conclusions [...] subject to suspension of the proceedings and referral to the Constitutional Court of the preliminary issue of constitutional legitimacy, considered relevant and not manifestly unfounded, of Article 9 of Law no. 108/1968 and Article 2, paragraph 6, of Legislative Decree no. 82/2005, for breach of Articles 2, 3, 48 and 49 of the Constitution".

DIGITAL MARKETS

1 May 2024 - Published in the Official Journal of the European Union the Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

Three years after its initial proposal in June 2021, the European Regulation known as eIDAS 2.0 has been published in the Official Journal of the European Union (EU Regulation 2024/1183) and marks a significant evolution in the EU's digital framework. It will enter into force on 20 May 2024, but will be applicable - as the case may be - in May 2026 or May 2027.

The highlights of the Regulation (which supplements and updates the previous Regulation 910/2014) are:

the introduction of the EU Common Digital Identity Wallet (EUDIW), which will be released free of charge (software components for wallet applications will be open source) and will enable EU citizens (on a voluntary basis and without discrimination if they choose not to join) to securely store and manage their data and official documents (such as identity cards, driving licences, diplomas, bank details, travel cards, etc.) and facilitate online interactions with other EU citizens.) and facilitate online interactions with authorities, businesses and citizens in all EU Member States;

- greater interoperability of digital identification systems between Member States and stronger security measures are introduced, with the introduction of more stringent authentication methods and enhanced security standards to increase trust in digital transactions and to promote a more secure digital marketplace in the EU;

- new trust services such as electronic attestation of attributes, electronic storage or electronic records are introduced. The Commission will establish a list of standards to be used by the end of 2024;

- the scope of qualified certificates for website authentication is clarified, to enable users to verify in a certified manner who administers websites and platforms (these certificates were already provided for in the 2014 eIDAS Regulation).

---

19 April 2024 - The European Commission published an overview of the European Union's Data Act, with information about its objectives and how it will work in practice.

The EU Regulation 2854/2023 (*Data Act*) officially entered into force on January 11th, 2024. It introduces harmonized rules on fair access to and use of data, in particular related to connected devices. It shall become operable on September 12nd, 2025.

The EU Commission provided this set of practical guidelines on how the Data Act gives users of connected products greater control over the data they generate while maintaining incentives for those who invest in data technologies. It also lays down general conditions for situations where a business has a legal obligation to share data with another business.

Specifically, the overview provides information on the following issues: **(1)** business-to-business and business-to-consumer data-sharing in the context of the Internet of things; **(2)** business-to-business data-sharing; **(3)** unfair contractual terms; **(4)** business-to-government data-sharing; **(5)** switching between data processing services; **(6)** unlawful third-country government access to data; **(7)** interoperability; and **(8)** enforcement.

As further development, the EU Commission anticipated a set of model contractual terms to help businesses conclude data-sharing contracts that are fair, reasonable, and non-discriminatory. These terms will also provide guidance on reasonable compensation and the protection of trade secrets.

Regarding the cloud, the EU Commission also will recommend a set of non-binding standard contractual clauses for cloud computing contracts between cloud service users and providers. An expert group has been set up to help the EC draft such terms and clauses, and it plans to recommend them by autumn 2025.

Within three years of its entry into application, the EC will carry out an evaluation of the impact of the Data Act, and, if necessary, may propose amendments.

COMPUTER CRIMES

5 April 2024 - Supreme Court of Cassation: computer fraud, the concept of 'digital identity' also applies in cases of home banking.

The notion of digital identity, which integrates the aggravating circumstance pursuant to Article 640-*ter*, third paragraph of the Criminal Code, does not presuppose a validation procedure adopted by the PA, but also finds application in cases of use of access credentials to private computer systems.

The defendant was sentenced by the Court for the offence of money laundering, for having made available to unknown persons his bank account where money from the offences of unauthorised access to a computer system and computer fraud had flowed. The Court of Appeal, partially reforming the first instance sentence, qualified the act under Article 640-ter of the criminal code and redetermined the sentence in favour of the man.

The defendant thus appealed to the Court of Cassation, claiming violation of the law and defective motivation with regard to the existence of the aggravating circumstance pursuant to paragraph 3 of Article 640-ter of the criminal code. He points out that the trial results do not prove the existence of theft or undue use of the digital identity, a concept that cannot be adapted to the case under examination, in which, in order to access the victim's bank account, an electronic key had been used to communicate the access code to be used from time to time.

In ruling No. 13559 of 3 April, the Second Criminal Section rejected the appeal.

The notion of digital identity, which integrates the aggravating circumstance in question, is not restricted to the validation procedures adopted by the PA, but also applies in the case of the use of access credentials to computer systems managed by private individuals.

In fact, the legislator has not provided any definition of digital identity.

The doctrine has pointed out that the translation into criminal law of definitions taken from external sources finds an obvious obstacle in the fact that they are conceptualisations or methodological indications functional to the specific measures to which they pertain.

The Office of the Attorney General has stated that 'digital identity is commonly understood as the set of information and resources granted by a computer system to a particular user of that system under an identification process (...)'.

Although it is, therefore, a concept destined to be defined in the future, the defence's argument that claims to limit digital identity only to validation procedures adopted by the PA duly certified cannot be accepted, excluding access procedures by means of credentials to privately managed computer systems such as home banking services or online sales platforms.

And these indications, expressed with regard to the use of personal credentials for access to so-called home banking systems or similar, can also be applied to the illegitimate use of so-called PINs and electronic keys that produce a code to perform the banking transaction, since in all cases, what matters is that 'the access

data to the computer system from time to time compulsorily entered by the agent directly or through the use of electronic devices, uniquely and uniquely identify a particular person by means of numbers or letters according to a unique sequence intended to be used (. .) only by the holder or a person authorised by him'.

Finally, it can be confirmed that the unauthorised use of the electronic key belonging to the account holder integrates the contested aggravating circumstance and presupposes, however, upstream, an unauthorised use of the account access credentials inherent in the person of its holder.

ELECTRONIC COMMUNICATIONS

28 April 2024 - Legislative Decree amending the Italian Electronic Communications Code. - On 28 April 2024, Legislative Decree 48/2024 amending the Electronic Communications Code (Legislative Decree 259/03) came into force. The new amendments (8 articles and 2 annexes) aims to update the text to technological innovation (also by introducing new definitions, such as that of "*access point*" or "*MAC Address*") and to standardise and simplify the regulations in various areas (from the SCIA procedure, to the mapping of electronic communication infrastructures, to the procedures for the installation of IT systems). The amendments introduced to section 98-*decies* of the Code are of a particular interest, with the provision of the possibility for the Italian Communications Authority - AGCOM to impose restrictions to block communications coming from abroad that illegitimately use national numbering to identify their origin, such as call centres, or to block sites that provide APP, software systems or illegitimate services, e.g. cashfor sms (illegitimate remuneration of end users of other operators), creation of parallel networks (dark web) that can also be used for illegal activities (copyright infringement, violation of privacy, child pornography, identity theft).