FIVERS

Regulatory update
Data protection, AI, IT and IP

n. 5 / 2024

DATA PROTECTION

1 July 2024 - EU Court of Justice: in the event of theft of personal data (even if not unlawfully used), the parties - private or public - who hold the data must also pay compensation.

---

27 June 2024 – Italian Data Protection Authority: proceedings started against 18 Regions and 2 Autonomous Provinces for corrective actions regarding the Electronic Health Record – FSE 2.0.

---

20 June 2024 - EU Court of Justice: an award of damages for processing under Article 82 of the GDPR does not necessarily have to be aggravated by a simultaneous breach of other regulations (such as those on professional regulation), although the judge remains free to decide on a case-by-case basis.

ARTIFICIAL INTELLIGENCE.

25 June 2024 - ESMA provides guidance to firms using artificial intelligence in investment services.

---

21 June 2024 – EU Commission hosts high-level meeting for the upcoming EU's AI Board to drive Ai Act implementation forward.

---

20 June 2024 - EU Commission: targeted public consultation on Artificial Intelligence in the financial sector launched.

DIGITAL MARKETS.

3 July 2024 – EU Commission sends preliminary findings to Meta over its "Pay or Consent" model for breach of the Digital Markets Act.

---

24 June 2024 - EU Commission v Apple, App Store Infringes the Digital Markets Act (EU Regulation 2022/1925).

---

18 June 2024 - EU Commission: published the report on the status of implementation in Member States of Directive 2019/2161 on the modernization and strengthening of online consumer protection.

INFORMATION TECHNOLOGY

2 July 2024 - Supreme Court of Cassation: WhatsApp messages constitute correspondence even if they have already been read and stored by the addressee and the rules on seizure of correspondence apply to them.

---

25 June 2024 - United Sections of the Court of Cassation: clarifying principles on the acquisition as evidence through a European Investigation Order from a foreign judicial authority of data taken from cryptophones.

CYBERSECURUTY

3 July 2024 - Cybersecurity Law no. 90/2024 published in the Official Gazette.

---

3 July 2024 – Italian Cybersecurity Agency: the new Regulation on cloud services for the public administration adopted and in force starting from August 1st, 2024.

---

27 June 2024 - EU Commission Delegated Regulations implementing certain obligations of the DORA Regulation published in the Official Journal of the EU.

COMPUTER CRIMES

21 June 2024 – Revenge porn: dissemination of the material must be carried out only by the person who took the footage or misappropriated it.

DATA PROTECTION

1 July 2024 - EU Court of Justice: in the event of theft of personal data (even if not unlawfully used), the parties - private or public - who hold the data must also pay compensation.

Scalable Capital, a company under German law, operated a 'trading app' in which the plaintiffs had opened an account. To that end, the latter saved certain personal data to their respective accounts, in particular their name, date of birth, postal address, email address and a digital copy of their identity card, and then paid a sum of several thousand euros to open those accounts.

The personal data as well as the data relating to the applicants' securities portfolio were then stolen by third parties whose identity remained unknown. Furthermore, it was not established whether or not the aforementioned personal data had been subject to fraudulent use.

Against this background, the applicants brought an action before the Amtsgericht München (District Court, Munich, Germany), the referring court, seeking compensation for the intangible damage they claimed to have suffered as a result of the theft of their personal data.

The EU Court of Justice provided new criteria for the interpretation and application of Article 82 of the GDPR on damages, confirming first of all that the right to compensation under that provision has an exclusively compensatory function and that monetary compensation based on that provision must allow full compensation for the damage suffered.

The Court also clarifies that in order to constitute and give rise to a right to compensation for immaterial damage within the meaning of Article 82 of the GDPR, the concept of 'identity theft' implies that the identity of a person affected by the theft of personal data is actually usurped by a third party. However, compensation for immaterial damage caused by the theft of personal data cannot be limited to cases where it is proven that such a data theft subsequently resulted in identity theft or usurpation. Therefore, data theft that has not yet been used to actually replace the data subject is also compensable.

On the basis of the principles provided by the EU Court, moreover, not only the perpetrators of the data theft are obliged to pay compensation, but also the private public entities that suffered the data breach and exfiltration, and this subjective widening of the range of obliged entities implies strong financial impacts. While it is true that the Court recalls that the sentence to pay compensation must not take on a punitive or exemplary character, it is equally true that in the context of determining the amount due by way of compensation for immaterial damage, the damage caused by a personal data breach is, by its very nature, no less serious than a personal injury.

---

27 June 2024 – Italian Data Protection Authority: proceedings started against 18 Regions and 2 Autonomous Provinces for corrective actions regarding the Electronic Health Record – FSE 2.0.

There is an urgent need to take action to protect the rights of all Italian patients involved in the processing of health data carried out through the Electronic Health Record 2.0.

With this motivation, the Italian Data Protection Authority has notified 18 Regions and the Autonomous Provinces of Bolzano and Trento of the initiation of corrective and sanctioning procedures for the numerous violations found in the implementation of the new rules on the FSE 2.0, introduced with the Ministry of Health decree of 7 September 2023.

In the previous days, the serious situation and the urgency of corrective action had been reported to the Prime Minister and the Minister of Health.

The results of the investigative activity on the ESF, which had begun at the end of January, showed that 18 Regions and the two Autonomous Provinces of Trentino Alto Adige - not being in line with the contents of the decree of 7 September 2023 - had modified, even significantly, the information model prepared by

the Ministry, subject to the opinion of the Italian Data Protection Authority, which should have been adopted throughout the country.

The discrepancies found have made it clear that certain rights (e.g. blackout, proxy, specific consent) and measures (e.g. security measures, differentiated levels of access, data quality) introduced by the decree, precisely for the protection of patients, are not guaranteed uniformly throughout the country. Or they are only exercisable and enforceable by patients in certain Regions and Autonomous Provinces, with a potentially significant discriminatory effect on patients.

This lack of homogeneity also contradicts the spirit of the ESF 2.0 reform aimed at introducing homogeneous measures, guarantees, and responsibilities throughout the country, thus also risking compromising the functionality, interoperability, and efficiency of the ESF 2.0 system.

The violations committed by the Regions and Autonomous Provinces, with different levels of seriousness and responsibility, may lead to the application of the sanctions provided for by the GDPR.

---

20 June 2024 - EU Court of Justice: an award of damages for processing under Article 82 of the GDPR does not necessarily have to be aggravated by a simultaneous breach of other regulations (such as those on professional regulation), although the judge remains free to decide on a case-by-case basis.

The case concerned some German taxpayers who had approached an accountant for their tax returns. The latter had sent the paper package by mail, but to the wrong address, leading to a situation whereby unauthorised third parties had gained access to the taxpayers' tax data who then sued the accountant for damages.

To the various questions posed by the referring court, the CJEU replied as follows.

First, a breach of the GDPR is not sufficient in itself to establish a right to compensation under Article 82. The data subject must also prove the existence of damage caused by that breach, without, however, that damage having to reach a certain degree of severity.

Secondly, the Court clarifies that a person's fear that his or her personal data, due to a breach of the GDPR, have been disclosed to third parties, without it being possible to prove that this was actually the case, is sufficient to give rise to a right to compensation provided that this fear, with its negative consequences, is duly proven.

Finally, in order to determine the amount due by way of compensation for a damage based on Article 82 of the GDPR

- the criteria for determining the amount of administrative fines laid down in Article 83 of the GDPR must not be applied mutatis mutandis;
- the right to compensation should not be given a deterrent function;
- no account is to be taken of simultaneous breaches of national provisions relating to the protection of personal data which do not have the object of clarifying the rules of the GDPR.

ARTIFICIAL INTELLIGENCE.

25 June 2024 - ESMA provides guidance to firms using artificial intelligence in investment services.

The European Securities and Markets Authority (ESMA), the EU's financial markets regulator and supervisor, issued a Statement providing initial guidance to firms using Artificial Intelligence technologies (AI) when they provide investment services to retail clients.

When using AI, ESMA expects firms to comply with relevant MiFID II requirements, particularly when it comes to organisational aspects, conduct of business, and their regulatory obligation to act in the best interest of the client.

Although AI technologies offer potential benefits to firms and clients, they also pose inherent risks, such as:

- Algorithmic biases and data quality issues;
- Opaque decision-making by a firm's staff members;
- Overreliance on AI by both firms and clients for decision-making; and
- Privacy and security concerns linked to the collection, storage, and processing of the large amount of data needed by AI systems.

Potential uses of AI by investment firm which would be covered by requirements under MiFID II include customer support, fraud detection, risk management, compliance, and support to firms in the provision of investment advice and portfolio management.

ESMA and the National Competent Authorities (NCAs) will keep monitoring the use of AI in investment services and the relevant EU legal framework to determine if further action is needed in this area.

---

21 June 2024 – EU Commission hosts high-level meeting for the upcoming EU's AI Board to drive Ai Act implementation forward.

Although still awaiting its formal entry into force of the AI Act, expected for early August, the meeting was gathered to set the groundwork for the forthcoming implementation of the AI Act.

The meeting underlined the need for early collaboration on the impending AI Act. The agenda featured discussions including:

- strategic vision on the implementation of the AI Act and the role of the Board
- national approaches to AI Act governance and supervision,
- first deliverables and priorities related to the AI Act's implementation by the European Commission
- organisation of the Board, such as its mandate, the process for selecting a Chair, decision making process and the creation of sub-groups.

Along with delegates from the European Commission high-level delegates from all EU Member States were present. The European Data Protection Supervisor (EDPS) attended in its observer role on the AI Board. Moreover, representatives from EEA/EFTA members—Norway, Liechtenstein, and Iceland—were also present in an observing capacity.

With the timing of the meeting the Commission and Member States aim to ensure a robust and timely setup for the AI governance framework, facilitating effective participation of Member States and implementation of the AI Act from day one. The next meeting will be held after the AI Act's entry into force, in the early Autumn.

The key provisions related to the establishment and tasks of the AI Board are Article 65 and 66 of the AI Act.

---

20 June 2024 - EU Commission: targeted public consultation on Artificial Intelligence in the financial sector launched.

The European Commission Directorate-General for Financial Stability, Financial Services, and Capital Markets Union requested public comments on artificial intelligence (AI) in the financial sector.

In particular, the consultation highlights that the EU AI Act aims to complement already existing financial service regulations and that the consultation intends to inform the Commission on the impact of AI in financial services, rather than create duplicative requirements.

Firstly, the consultation considers the AI applications in financial services, including particular use cases such as fraud detection, risk management, automation of routine tasks, personalized financial advice, enhanced decision-making, and improved customer services. The consultation further seeks clarification on the challenges and risks of the use of AI applications such as regulatory compliance with financial regulations, bias and discrimination, transparency and explainability, and dependability. More specifically, the consultation seeks clarification on general-purpose AI (GPAI) in financial services, pursuant to the definition given under Article 3(63) of the AI Act.

In addition, the consultation considers specific use cases of AI in financial services. This includes the use of AI in banking and payments and the use of AI for AI credit risk assessment and credit scoring, compliance, anti-money laundering, and customer service. Similarly, the consultation seeks information on the use of AI in securities markets for risk assessments and possible uses of AI in insurance and pensions.

Finally, the consultation seeks further information on AI and financial services in the specific context of the AI Act. Notably, the consultation highlights that the AI Act establishes two high-risk use cases for the financial sector, namely where AI systems are intended to be used to evaluate the creditworthiness of natural persons or establish their credit score and where AI systems are intended to be used for risk assessment and pricing for natural persons in the case of life and health insurance. Accordingly, the consultation requests feedback on the need for appropriate guidance to implement the above provisions.

Public comments may be submitted here until September 15, 2024.

DIGITAL MARKETS.

3 July 2024 – EU Commission sends preliminary findings to Meta over its "Pay or Consent" model for breach of the Digital Markets Act.

The Commission has informed Meta of its preliminary findings that its "pay or consent" advertising model fails to comply with the Digital Markets Act (DMA). In the Commission's preliminary view, this binary choice forces users to consent to the combination of their personal data and fails to provide them a less personalised but equivalent version of Meta's social networks.

Online platforms often collect personal data across their own and third party services to provide online advertising services. Due to their significant position in digital markets, gatekeepers have been able to impose terms of services on their large user base allowing them to collect vast amounts of personal data. This has given them potential advantages compared to competitors who do not have access to such a vast amount of data, thereby raising high barriers to providing online advertising services and social network services.

Under Article 5(2) of the DMA, gatekeepers must seek users' consent for combining their personal data between designated core platform services and other services, and if a user refuses such consent, they should have access to a less personalised but equivalent alternative. Gatekeepers cannot make use of the service or certain functionalities conditional on users' consent.

---

24 June 2024 - EU Commission v Apple, App Store Infringes the Digital Markets Act (EU Regulation 2022/1925).

The EU Commission informed Apple that the App Store rules breach the Digital Markets Act (DMA), as they prevent app developers from freely directing consumers to alternative channels for offers and content.

In addition, the EU Commission started a new non-compliance proceedings against Apple due to concerns that its new contractual requirements for third-party app developers and app stores, including Apple's new *'Core Technology Fee'*, fail to ensure effective compliance with Apple's obligations under the DMA.

According to the DMA, developers who distribute their apps via Apple's App Store should be able, free of charge, to inform their customers about cheaper alternative purchase options, direct them to such offers, and allow them to make purchases.

Apple currently has three categories of commercial terms governing its relationship with app developers, including App Store address rules. The EU Commission notes at the outset that:

- none of these commercial terms allow developers to freely guide their customers. In particular, developers cannot inform customers of prices within the app or otherwise communicate with their customers to promote offers available on alternative distribution channels;
- in most of the terms of business available to app developers, Apple allows guidance only through 'link-out', i.e., app developers may include in their app a link that redirects the customer to a web page where the customer can conclude a contract. The link-out process is subject to numerous restrictions imposed by Apple that prevent app developers from communicating, promoting offers and concluding contracts through the distribution channel of their choice.
Although Apple may receive a fee for facilitating the initial acquisition of a new customer by developers via the App Store, the fees charged by Apple go beyond what is strictly necessary for such a fee.

Apple now has the opportunity to exercise its rights of defence by examining the documents contained in the European Commission's investigation file and responding in writing to the executive's preliminary findings.

If the Commission's preliminary findings are confirmed, the Commission will adopt a non-compliance decision within 12 months of the opening of the proceedings (25 March 2024).

---

18 June 2024 - EU Commission: published the report on the status of implementation in Member States of Directive 2019/2161 on the modernization and strengthening of online consumer protection.

The European Commission has published a report on the implementation of Directive 2019/2161 on better enforcement and modernization of the Union's consumer protection rules, which has introduced significant updates to existing legislation, especially regarding:

- bans on unfair online practices such as advertising and paid placements in search results;
- new transparency requirements regarding the placement of online search results and the conclusion of a contract in an online marketplace; and
- the extension of the Consumer Rights Directive to free digital services for which consumers provide personal data rather than monetary compensation.

In particular, the report highlighted gaps in the national implementation of transparency rules on search results. In addition, it was noted that rules requiring online search service providers that include advertisements in search results to ensure that they are clearly visible and easily distinguishable from other search results should be better enforced. The report mentioned that in the case of large online platforms (VLOPs) and large online search engines (VLOSEs), the Digital Services Act (DSA) requires the availability of at least one non-personalized recommendation system option.

In addition, the report found that online marketplaces have implemented a requirement to provide additional information about the status of third-party vendors, but that consumers are still unsure of the identity of the vendors and how the transaction will take place.

Finally, although several EU member states have implemented new options to allow consumers to withdraw consent in transactions based on the provision of personal data, there is still no measurement of the impact of these practices.

INFORMATION TECHNOLOGY

2 July 2024 - Supreme Court of Cassation: WhatsApp messages constitute correspondence even if they have already been read and stored by the addressee and the rules on seizure of correspondence apply to them.

With ruling no. 25549 of 28 June 2024, the Supreme Court of Cassation applied for the first time the new orientation expressed by the Constitutional Court in ruling no. 170 of 2023 and clarified whether WhatsApp messages, after having been read and retained by the addressee, must be acquired in compliance with the discipline of interception of computer or telematic communications or that of seizure of correspondence or that of simple documents.

Until the pronouncement of the Constitutional Court (which ruled that making WhatsApp messages lose the nature of correspondence only because they were read would restrict the scope of constitutional protection under Article 15 of the Constitutional Constitution), the Supreme Court followed a course of action that reconducted the messages of the social read and stored as mere documents, making Article 234 of the Code of Criminal Procedure applicable, stating that: "on the subject of evidence, e-mail messages WhatsApp messages and SMS messages stored in the memory of an electronic device retain the nature of correspondence even after receipt by the addressee, at least until the passage of time for another cause they have lost all character of actuality, in relation to the interest and its confidentiality, turning into a mere historical document so that - until that time - their acquisition must take place according to the forms provided by art. 254 cod. proc. penal for the seizure of correspondence".

---

25 June 2024 - United Sections of the Court of Cassation: clarifying principles on the acquisition as evidence through a European Investigation Order from a foreign judicial authority of data taken from cryptophones.

The United Criminal Sections of the Court of Cassation in its judgment No. 23755 of 14 June 2024 answered the following questions: "Does the acquisition of messages on group chats, exchanged using an encrypted system, by means of a European Investigation Order with a foreign judicial authority that has carried out the decryption constitute the acquisition of computer documents and data within the meaning of Article 234-bis of the Code of Criminal Procedure or of documents pursuant to Article 234 of the Code of Criminal Procedure? 234 of the Code of Criminal Procedure, or is it subject to other rules relating to the acquisition of evidence; whether the acquisition referred to above must be subject, for the purposes of the usability of the relevant data, to prior or subsequent judicial verification of its legitimacy by the national judicial authority".

These are the principles of law affirmed by the Supreme Court:

- the transmission, requested by means of a European investigation order, of the content of communications exchanged by means of crypto-mobile telephones, already acquired and decrypted by the foreign judicial authority in criminal proceedings pending before it, does not fall within the scope of Article 234-bis of the Code of Criminal Procedure, which operates outside the hypotheses of cooperation between judicial authorities, but rather within the rules relating to the circulation of evidence between criminal proceedings, as inferable from Articles 238 and 270 of the Code of Criminal Procedure and 78 of the operative provisions of the Code of Criminal Procedure

- with regard to the European Investigation Order, evidence already in the possession of the competent authorities of the executing State may be legitimately requested and acquired by the Italian Public Prosecutor without the need for prior authorisation by the judge of the proceedings in which it is intended to be used

- the issuance, by the Public Prosecutor, of a European Investigation Order aimed at obtaining the content of communications exchanged by means of crypto-mobile telephones, already acquired and decrypted by

the foreign judicial authority in criminal proceedings pending before it, does not need to be preceded by authorisation from the Italian court, as a necessary condition under Article 6 of Directive 2014/41/EU, because such authorisation, under the national rules on the circulation of evidence, is not required in order to obtain the availability of the content of communications already acquired in other proceedings

- the rules set out in Article 132 of the Privacy Code relating to the acquisition of data concerning electronic communications traffic and the location of the devices used, apply to requests addressed to service providers, but not to those addressed to another judicial authority that already holds such data, so that, in this case, the public prosecutor may legitimately access them without seeking prior authorisation from the judge before whom he intends to use them

- the usability of the content of communications exchanged by means of crypto-mobile telephones, already acquired and decrypted by the foreign judicial authority in criminal proceedings pending before it, and transmitted on the basis of a European Investigation Order, must be excluded if the Italian court finds that their use would give rise to a breach of fundamental rights, it being understood that the burden of alleging and proving the facts from which to infer such a breach rests on the party concerned

- the impossibility for the defence to have access to the algorithm used within a system of communications to encrypt the text of those communications does not give rise to a violation of fundamental rights, since the danger of alteration of the data must be excluded, unless specific allegations to the contrary are made, since the content of each message is inseparably linked to its encryption key, and an incorrect key has no possibility of decrypting it even partially.

CYBERSECURUTY

3 July 2024 - Cybersecurity Law no. 90/2024 published in the Official Gazette.

Law of June 28th, 2024 no. 90 has been published in the Official Italian Gazette n. 153.

The text consists of 24 articles that introduce, among other changes:

- harsher penalties for crimes such as abusive access to a computer system or damaging computer information, data and programs;
- a broadening of the scope of those required to strengthen their defenses;
- new crimes such as computer extortion;
- lengthening of investigation time and the use of wiretaps is encouraged;
- the centrality, for the most serious crimes, of the Anti-Mafia Prosecutor's Office;
- an alert procedure and collaboration with Acn, the cyber security agency, for remedial action;
- a mode of intervention when there are competing competencies, for example, of Acn and the judicial police;
- strengthening action against cyber crimes, with the identification of new offenses and the use of more effective investigative tools.

Among the various new features is also the introduction of a 3 paragraph in Article 629 of the Criminal Code (extortion), which in turn is referred to in Article 24-bis Legislative Decree no. 231/2001 on the subject of the liability of entities, according to which "anyone who, through the conduct referred to in Articles 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater and 635-quinquies or with the threat of performing them, compels someone to do or omit something, procuring for himself or others an unjust profit to the detriment of others, shall be punished by imprisonment of from six to twelve years and a fine of from 5,000 to 10,000 euros. The punishment shall be imprisonment from eight to twenty-two years and a fine from 6,000 euros to 18,000 euros, if any of the circumstances indicated in the third paragraph of Article 628 concur, as well as in the case where the act is committed against a person incapacitated by age or infirmity."

---

3 July 2024 – Italian Cybersecurity Agency: the new Regulation on cloud services for the public administration adopted and in force starting from August 1st , 2024.

Digital services are the primary means of delivering services to citizens by Public Administrations. The transition journey to the PA cloud ensures reliability, security, and long-term sustainability of public services.

The **qualification** process allows the Agency to perform pre-checks on the compliance level of cloud services offered by private operators, which Public Administrations can use as an alternative to self-providing services.

The selection of cloud services qualified by ACN is based on the classification of data and services of Public Administrations. Through this classification, the impact of services and data handled by a Public Administration is determined relative to their level of criticality.

Public Administrations can consult the ACN Catalogue to verify qualified services and the granted qualification level, to proactively determine if they conform to the required classification level for managing their data or services.

The ACN Unified Regulation for digital infrastructures and cloud services for the Public Administration clarifies

- the methods for **classification**, **migration** and **qualification of cloud services**, which the PA can procure via open market;
- the measures and requirements for achieving **minimum levels** of security, computing capacity, energy efficiency, and reliability of digital infrastructures for the PA;
- the quality, security, performance, scalability, and portability **characteristics** of cloud services for the PA..

The Regulation, adopted by ACN through Directorate Decree n. 21007/24 of 27 june 2024 and applicable from August 1, 2024, updates the minimum levels and characteristics in response to the changing risk landscape and the terms related to the qualification issuance process. The Regulation also governs the use of **housing infrastructures** and **proximity services** (so-called edge services), increasingly prevalent due to the need to reduce latency times for end users
One of the main novelties also involves differentiation between:

- the **qualification** of cloud services provided by private suppliers, which requires a pre-verification of compliance followed by the publication of the corresponding data card on the ACN Catalogue,
- the **adaption** of infrastructures (regardless of the nature of the responsible entities) and services provided by public operators, based on a declaration of conformity submitted to ACN according to the specified requirements.

In both cases, a post-validation monitoring phase is scheduled during the 36-month validity period of the qualification and adaptation, enabling ACN to verify the maintenance of requirements necessary for data and service processing, in accordance with the classification level.
As of 1 August 2024, cloud service infrastructures that had obtained a valid QI1-4 level qualification will be converted - as far as the nomenclature is concerned - to AI1-4 level.

---

27 June 2024 - EU Commission Delegated Regulations implementing certain obligations of the DORA Regulation published in the Official Journal of the EU.

The following delegated acts implementing EU Regulation 2022/2554 on digital operational resilience (DORA Regulation) have been published in the Official Journal of the European Union:

- **Delegated Regulation (EU) 2024/1772** on criteria for the classification of cyber incidents
- Delegated Regulation (EU)**2024//1773** on the policy for the provision of ICT services by third parties in support of essential or important functions

- Delegated Regulation (**EU) 2024/1774** on IT risk management tools, methods, processes and policies

The delegated regulations will enter into force on 15 July 2024, be mandatory in all their elements and directly applicable.

Many financial, banking and insurance entities required - as of 17 January 2025 - to implement EU Regulation 2022/2554 on Digital Operational Resilience (DORA Regulation) are required to review many internal management policies. For example, Chapter V with only three articles (28-30) redesigns and profoundly impacts the procedures for selecting and qualifying ICT suppliers and the very structure of contracts with third-party ICT suppliers and their lifecycle. Moreover, the DORA Regulation obliges to update roles, organisational charts and directives to personnel, impacts training plans - to be diversified according to management or non-management role - rewrites the responsibilities of statutory auditors and, above all, places the management body at the centre of the responsibility system. The publication in the Official Journal - last 25 June - of the above-mentioned delegated acts of the EU Commission (among other things, the overall framework, including DORA, Regulatory Technical Standard - RTS between January and July 2024 and delegated acts of extraordinary complexity and articulation) confirms the need to coordinate DORA requirements with other existing policies. The deep intertwining between the DORA Regulation and the GDPR, for example: not only does the DORA Regulation insist on obligations to ensure '*authenticity, integrity, confidentiality and availability*' of both personal and non-personal data, but the same delegated acts now published regulate the impact of DORA fulfilments on GDPR compliance policies already in place. For example, Delegated Regulation (EU) 2024/1772 on criteria for classifying IT incidents sets out the relationship with GDPR *data breach* notification in the event of an incident; or the Delegated Regulation (EU) 2024//1773 on the policy for the provision of ICT services by third parties in support of '*essential or important functions*' reminds that in case the provider is also an external *Data Protection* Officer under the GDPR, the *data protection* requirements are to be included in the policy, which (see e.g. Art. 5, paragraph 3, letter (e) of the GDPR) must also include a specific preliminary risk assessment on the provider with regard to "risks related to the protection of confidential or personal data" (an assessment that also the Guidelines of the European Data Protection Board no. 7/2020 on the concept of controller and processor require to be carried out on the external provider-processor).

COMPUTER CRIMES

21 June 2024 – Revenge porn: dissemination of the material must be carried out only by the person who took the footage or misappropriated it.

The dispute under review concerns the crime of unlawful dissemination of sexually explicit images or videos under Article 612-ter of the Criminal Code, commonly referred to using the expression "revenge porn."

Titius appeals in cassation, censuring the judgment under appeal, arguing that the dissemination "must take place without the consent of the persons represented and must concern sexually explicit materials intended to remain private, but, as repeatedly noted, consensually made, so much so that the conduct can only be carried out by the person who operated the filming or by the person who wrongfully took possession of it, removing it from the person who had made it."

In the case at hand, on the other hand, the filming had been the result of environmental wiretapping carried out by the prosecutor's office without the full knowledge of the subjects filmed, so that, subject to the violation of the principle of legality and taxability, it cannot be considered in the same way as the material indicated by the first and third paragraphs of Article 612-ter of the Criminal Code.

In the field of legitimacy, the Supreme Court of Cassation, Criminal Sect. V, in its ruling of June 20, 2024, No. 24379 first of all traces the phenomenon of "revenge porn," to which our Legislature responded with the introduction in the Criminal Code of Article 612-ter, approved by an amendment to Law No. 69/2019, the so-called "Red Code."

As emerges from the normative text, "the norm not only requires the absence of consent, but also that the images or videos are 'intended to remain private,' as if, it has been observed in doctrine, even before the absence of consent to disclosure, there is the rupture of a pactum fiduciae between two individuals, presumably linked by a relationship, such as to have imprinted a precise destination to the contents, later disregarded by one of the two."

As for the ground of appeal specified above, the Supreme Court finds it well-founded.

By virtue of the hermeneutic evolution of the conduct and the latitude of the syntagma revenge porn, the Court considers that the incriminated conduct is broader than that carried out solely in the context of a previous romantic relationship, in the context of which a different use of the material originally intended to remain circumscribed and confidential occurred. The rubric of the rule, which outlines the criminal relevance of the unlawful dissemination of sexually explicit images and videos, without any reference to a specific context of a prior romantic relationship, lends support to this orientation.

That being said, the Supreme Court reiterates the two requirements that must both exist simultaneously: lack of consent and private purpose, understood as the formation of the material by the same individuals depicted in it. Therefore, it is necessary that the perpetrator of the conduct of dissemination of the said material be the one who had previously made the said material, or had taken possession of it by misappropriating it.

These requirements do not appear to be met in the present case, since the perpetrator is a person entirely different from the one who had made the material, nor does it appear that he had appropriated it by misappropriating it.

For these reasons, the Supreme Court upholds the appeal.