FIVERS

# Regulatory update

## Data protection, IP, IT e AI

**n. 2 / 2024**

### DATA PROTECTION

**13 May 2024 - Supreme Court of Cassation: processing and selection of video material to analyse behaviour constitutes processing of biometric data within the meaning of Article 9 of the GDPR.**

---

**8 May 2024 - Supreme Court of Cassation: the removal of a video from the Internet also entails the obligation to take action on third-party portals.**

---

**3 May 2024 - Work: Italian Data Protection Authority: the employee has the right to access his/her personal data regardless of the reason for the request.**

---

**20 May 2024 - Vatican City State publishes General regulation on the protection of personal data.**

---

**8 May 2024 - Spanish Data Protection Authority: Guidelines published on the processing of personal data by tracking Wi-Fi systems.**

---

### ARTIFICIAL INTELLIGENCE.

**21 May 2024 – EU Council gives final green light to the Artificial intelligence (AI) act.**

---

**17 May 2024 - Council of Europe adopts first international treaty on artificial intelligence.**

---

**17 May 2024 – EU Commission compels Microsoft to provide information under the Digital Services Act on generative AI risks on Bing.**

---

### DIGITAL MARKETS.

**21 May 2024 – Council of State and Regional Administrative Court: Agcom sanctions against Google have been confirmed for having disseminated advertising of games with cash winnings on Google Search and YouTube, in contravention of the Dignity Decree.**

---

**13 May 2024 - EU Commission designates Booking as a gatekeeper under the Digital Markets Act - DMA (EU Regulation 2022/1925) and opens a market investigation into X.**

---

**12 May 2024 - EU Commission launches Whistleblower Tools for Digital Services Act and Digital Markets Act.**

## INFORMATION TECHNOLOGY

**6 May 2024 - Supreme Court of Cassation: certified electronic mail (PEC) is suitable for proving the sending and receipt of a message, but not for guaranteeing the content of the document attached to it.**

## DATA PROTECTION

### 13 May 2024 - Supreme Court of Cassation: processing and selection of video material to analyse behaviour constitutes processing of biometric data within the meaning of Article 9 of the GDPR.

The Court of Cassation, with Order No. 12967 of 13 May 2024, established relevant principles on what is to be understood as the processing of biometric data under Articles 4(14) and 9 of the GDPR. It upheld the Italian Data Protection Authority's appeal against a Court ruling that had annulled a decision of the Italian Data Protection Authority ruling out that there was no processing of biometric data in the mere video recording of students taking university examinations remotely, with software that analysed behaviour, taking photos and flagging those that highlighted any anomalous behaviour (e.g: attempt to copy), photos then collected in a video submitted to the evaluation of the teacher, established that this treatment represents a processing of biometric data since " *it is clear that video and photo recordings do not only have the function of documenting the examination test, but are characterised by the contextual processing and selection of the material collected, which converges in the identification and reporting of anomalous behaviour, through the production of the final video*". However, the broad interpretation (inter alia of a mandatory prohibition rule such as Article 9 of the GDPR) that identifies in this video recording processing all four phases of a biometric processing as indicated by the General Measure of the Privacy Guarantor on biometrics of 2014 (1. detection of biometric characteristics; 2) acquisition of a biometric sample; 3) extraction from the biometric sample, by means of mathematical processing, of characteristic traits suitable for constituting the biometric template; 4) comparison or matching for the unique identification of the natural person). Step 3 in particular seems to be missing. Among other things, the 'unambiguous identification' of the person should be the result, entirely automatic, of the biometric processing, whereas in the case of the software analysed by the Court of Cassation, the assertion that the University has identified the participants in the exam beforehand and therefore the video of the suspect student (whose identity the software does not know) is traced ex post by the teacher back to the person in question is not very supportable. Hence, data controllers and processors must pay particular attention to such image processing software-assisted video recording systems, as they could fall under the strict prohibitions of Article 9 GDPR. Such cases will become increasingly common with the AI Act, which contains many concepts related to biometrics (from 'biometric categorisation' to 'emotion recognition system' to 'biometric identification', in real time and ex post). But doubts remain.

### 8 May 2024 - Supreme Court of Cassation: the removal of a video from the Internet also entails the obligation to take action on third-party portals.

With Order no. 9068/2024, the Supreme Court of Cassation - dealing with a case involving the liability of a television production company for failing to restrict the dissemination of defamatory video material - confirmed the TV broadcaster's sentence to pay damages and recalled - also pursuant to Article 17 of Regulation 679/2016 ("GDPR") and the EU Court of Justice's case law in the 2013 *Google Spain* case - that the data controller has an obligation not only to delete personal data unlawfully processed through links pointing to a video, but also to take steps to remove the service and the news that reproduce it from search engines or third-party portals (such as YouTube), even if not directly dependent on him. The Court also specified that the owner must demonstrate and give evidence of his proactive approach in managing personal data protection issues, particularly when they are disseminated in critical contexts due to the possibility offered by the dissemination channel and web technology to amplify the harmful consequences of news dissemination. Also interesting is the jurisprudential reconstruction contained in this ordinance of the relationship between the right to criticism, the right to report news, the characteristics of so-called investigative journalistic activity and defamation profiles.

### 3 May 2024 - Work: Italian Data Protection Authority: the employee has the right to access his/her personal data regardless of the reason for the request.

This was reaffirmed by the Privacy Guarantor in upholding, in a decisive ruling, the complaint lodged by a woman who had asked the bank where she had been employed for access to her personal file in order to find out what information might have given rise to a disciplinary sanction against her.

The bank had failed to respond adequately to the request and had only provided an incomplete list of the documentation collected, omitting certain information on the basis of which the disciplinary sanction had been imposed.

It was only after the opening of the investigation by the Authority that the bank had handed over to the former employee the further documentation contained in the file.

This concerned, in particular, correspondence between the bank and a third person, who complained about the unlawful communication of confidential information of her husband, the current account holder, to the complainant, who had used it in the context of legal proceedings.

The bank, in its reply notes to the Authority, argued that it had not provided the former employee with this documentation in order to protect the right of defence and the confidentiality of the third parties involved, as well as because the complainant had no interest in access.

The Garante noted that, as a general rule, the purpose of the right of access is to enable the data subject to have control over his personal data and to verify their accuracy. This right, however, cannot be denied or limited depending on the purpose of the request. Indeed, according to the provisions of the Regulation, data subjects are not required to state a reason or a particular need to justify their requests to exercise their rights, nor can the data controller verify the reasons for the request. This interpretation has also been clarified by the European Data Protection Board (EDPB) through the approval of the Guidelines on the right of access and is the result of consistent case law of the Court of Justice.

In sanctioning the bank for EUR 20,000, the Authority took into account the nature, seriousness and duration of the violation, but also the absence of similar precedents.

---

**20 May 2024 - Vatican City State publishes General regulation on the protection of personal data.**

The Vatican City State published a decree promulgating the general regulation on the protection of personal data (the general data protection regulation).

In particular, the general regulation applies to the processing of personal data carried out by the Governorate of the Vatican City State, limited to the territory of the Vatican City State. Processing carried out for exclusively personal purposes, personal data manifestly made public, or anonymized data are not subject to the general regulation.

The general regulation provides, among other things:

- key definitions such as 'personal data,' 'processing,' and 'data controller,' as well as principles of lawfulness, correctness, transparency, good faith, and proportionality;
- conditions for processing of special categories of personal data and conditions for valid consent;
- responsibilities of the controller, including regarding the register of processing activities, engagement of a data processor, and implementation of suitable security measures;
- rights of the data subject, such as the right to information, access, rectification, erasure, object, data portability, and limit processing, as well as the procedure for exercising such rights; and
- designation of a data protection officer (DPO), including the right to launch a complaint with the DPO and subsequent evaluation by the President of the Governorate of the Vatican City State.

The general regulation immediately entered into force upon publication and for a three-year experimental period.

---

**8 May 2024 - Spanish Data Protection Authority: Guidelines published on the processing of personal data by tracking Wi-Fi systems.**

Wi-Fi localisation is a technology that allows mobile devices to be identified and tracked through the Wi-Fi signals they emit, to detect the presence of the device in a specific area and to identify movement

patterns, which is why it is used, for example, in capacity estimation, people flow analysis or the measurement of dwell times.

Practical applications can be found in shopping centres, museums, workplaces, public areas, public transport or large public events. However, this practice poses serious privacy risks, as it may allow people's movements to be tracked without their knowledge and without a proper legal basis.

Many of these uses of Wi-Fi tracking involve the collection and processing of personal data and are subject to Regulation 679/2016 ('GDPR'). With this in mind, the AEPD - the Spanish Data Protection Authority - has adopted The *Guidelines on the processing of personal data in the context of tracking via Wi-Fi technologies*, which analyse from a technical and legal perspective the data protection implications of the use of this technology, identifying the main risks and offering a series of concrete recommendations for a responsible use compatible with data protection regulations.

---

## ARTIFICIAL INTELLIGENCE.

### 21 May 2024 – EU Council gives final green light to the Artificial intelligence (AI) act.

On May 21st, 2024 the EU Council approved definitively the EU General Regulation on AI, aiming to harmonise rules on artificial intelligence, the so-called AI Act. The flagship legislation follows a 'risk-based' approach, which means the higher the risk to cause harm to society, the stricter the rules. It is the first of its kind in the world and can set a global standard for AI regulation. The new law aims to foster the development and uptake of safe and trustworthy AI systems across the EU's single market by both private and public actors. At the same time, it aims to ensure respect of fundamental rights of EU citizens and stimulate investment and innovation on artificial intelligence in Europe. The AI act applies only to areas within EU law and provides exemptions such as for systems used exclusively for military and defence as well as for research purposes.

---

### 17 May 2024 - Council of Europe adopts first international treaty on artificial intelligence.

The Council of Europe has adopted the first-ever international legally binding treaty aimed at ensuring the respect of human rights, the rule of law and democracy legal standards in the use of artificial intelligence (AI) systems. The treaty, which is also open to non-European countries, sets out a legal framework that covers the entire lifecycle of AI systems and addresses the risks they may pose, while promoting responsible innovation. The convention adopts a risk-based approach to the design, development, use, and decommissioning of AI systems, which requires carefully considering any potential negative consequences of using AI systems.

The Council of Europe Framework Convention on artificial intelligence and human rights, democracy, and the rule of law was adopted in Strasbourg during the annual ministerial meeting of the Council of Europe's Committee of Ministers, which brings together the Ministers for Foreign Affairs of the 46 Council of Europe member states.

The convention is the outcome of two years' work by an intergovernmental body, the Committee on Artificial Intelligence (CAI), which brought together to draft the treaty the 46 Council of Europe member states, the European Union and 11 non-member states (Argentina, Australia, Canada, Costa Rica, the Holy See, Israel, Japan, Mexico, Peru, the United States of America, and Uruguay), as well as representatives of the private sector, civil society and academia, who participated as observers.

The treaty covers the use of AI systems in the public sector - including companies acting on its behalf - and in the private sector. The convention offers parties two ways of complying with its principles and obligations when regulating the private sector: parties may opt to be directly obliged by the relevant convention provisions or, as an alternative, take other measures to comply with the treaty's provisions while fully respecting their international obligations regarding human rights, democracy and the rule of law. This approach is necessary because of the differences in legal systems around the world.

The convention establishes transparency and oversight requirements tailored to specific contexts and risks, including identifying content generated by AI systems. Parties will have to adopt measures to identify, assess, prevent, and mitigate possible risks and assess the need for a moratorium, a ban or other appropriate measures concerning uses of AI systems where their risks may be incompatible with human rights standards.

They will also have to ensure accountability and responsibility for adverse impacts and that AI systems respect equality, including gender equality, the prohibition of discrimination, and privacy rights. Moreover, parties to the treaty will have to ensure the availability of legal remedies for victims of human rights violations related to the use of AI systems and procedural safeguards, including notifying any persons interacting with AI systems that they are interacting with such systems.

As regards the risks for democracy, the treaty requires parties to adopt measures to ensure that AI systems are not used to undermine democratic institutions and processes, including the principle of separation of powers, respect for judicial independence and access to justice.

Parties to the convention will not be required to apply the treaty's provisions to activities related to the protection of national security interests but will be obliged to ensure that these activities respect international law and democratic institutions and processes. The convention will not apply to national defence matters nor to research and development activities, except when the testing of AI systems may have the potential to interfere with human rights, democracy or the rule of law.

In order to ensure its effective implementation, the convention establishes a follow-up mechanism in the form of a Conference of the Parties.

Finally, the convention requires that each party establishes an independent oversight mechanism to oversee compliance with the convention, and raises awareness, stimulates an informed public debate, and carries out multistakeholder consultations on how AI technology should be used. The framework convention will be opened for signature in Vilnius (Lithuania) on 5 September on the occasion of a conference of Ministers of Justice.

---

**17 May 2024 – EU Commission compels Microsoft to provide information under the Digital Services Act on generative AI risks on Bing.**

The Commission steps up its enforcement actions against Microsoft: after not having received an answer to its request for information from 14 March regarding specific risks stemming from Bing's generative AI features, notably 'Copilot in Bing' and 'Image Creator by Designer', the company now has until 27 May to provide the requested information to the Commission.

With this legally binding request for information, the Commission is asking Bing to provide internal documents and data that were not disclosed in Bing's previous response. The request for information is based on the suspicion that Bing may have breached the DSA for risks linked to generative AI, such as so-called 'hallucinations', the viral dissemination of deepfakes, as well as the automated manipulation of services that can mislead voters. Under the DSA, designated services, including Bing, must carry out an adequate risk assessment and adopt respective risk mitigation measures (Art 34 and 35 of the DSA). Generative AI is one of the risks identified by the Commission in its guidelines on the integrity of electoral processes, in particular for the upcoming elections to the European Parliament in June.

In case Bing fails to reply within the deadline, the Commission may impose fines up to 1% of the provider's total annual income or worldwide turnover and periodic penalties up to 5% of the provider's average daily income or worldwide annual turnover. The Commission can also impose fines up to 1% of the provider's total annual income or worldwide turnover for incorrect, incomplete, or misleading information in response to a request for information.

Following its designation as Very Large Online Search Engine, Bing is required to comply with the full set of provisions introduced by the DSA. In this particular case, the Commission considers that the suspected

violations of the DSA may present risks linked to civic discourse and electoral processes. According to Article 67(3) of the DSA, the Commission is empowered to request, by decision, further information to Bing relating to suspected infringements.

A request for information is an investigatory act that does not prejudge potential further steps the Commission may or may not decide to take. Based on the assessment of the replies, the Commission will assess the next steps. This could entail the opening of formal proceedings, pursuant to Article 66 of the DSA.

---

## DIGITAL MARKETS.

**21 May 2024 – Council of State and Regional Administrative Court: Agcom sanctions against Google have been confirmed for having disseminated advertising of games with cash winnings on Google Search and YouTube, in contravention of the Dignity Decree.**

The Council of State (with judgment no. 4277 of 13 May 2024 regarding the search engine service "Google Search") and the Regional Administrative Court of Lazio (with order no. 1940 of 16 May 2024, with regard to the video sharing service "YouTube") confirmed the sanctions that the Italian Communications Authority - AGCOM had imposed for violation of the prohibition on advertising games with cash winnings introduced by Article 9 of Decree-Law no. 87 of 12 July 2018, converted with amendments by Law no. 96 of 9 August 2018 ("*Dignity Decree*"). This is a fundamental case law (also in line with the judgment of the Supreme Court of Cassation no. 7708 of 19 March 2019 on the liability of providers) which for the first time recognized the liability of Google/YouTube for violation – through the provision of its *Google Ads service* – of the Dignity Decree. Google has therefore been considered by the administrative judges to be an *active hosting provider* (because – explains the Council of State – Google carries out a control over the content of the *Google Ads* service, in order to optimize its economic interests) and, therefore, directly responsible for the content promoted through this advertising service. The jurisprudential "reversal" is absolutely relevant because in a certain sense it contrasts with the previous ruling of the Court of Justice of the EU (of 23 March 2010 on case C-236/08) in which Google was considered a subject having a "*merely technical, automatic and passive*" function of the Google Ads service and therefore irresponsible in its qualification as *a passive hosting provider*. For the first time, a ruling establishes that those who host an advertisement on the Internet are not exempt from the responsibility of supervising the content. The principle supported by the ruling of the Council of State paves the way for the liability of platforms for any illegal advertising, including content that violates copyright, highlighting effects that in theory are announced as disruptive. The Council of State has established that the moment in which the platform necessarily becomes aware of the nature of the content (in some cases "*explicitly illicit*") coincides with the moment in which it accepted it to publish it (and not with the – subsequent – moment of notification by commercial partners and/or users). And this also appears to be in line with the rapid timeline for the removal of illegal content now provided for by the new legislation introduced by the Digital Services Act (EU Regulation 2022/2065).

---

**13 May 2024 - EU Commission designates Booking as a gatekeeper under the Digital Markets Act - DMA (EU Regulation 2022/1925) and opens a market investigation into X.**

The European Commission has designated Booking as a gatekeeper under the DMA for its online intermediation service Booking.com and decided not to designate X Ads and TikTok Ads. In parallel, the Commission has opened a market investigation to further assess the rebuttal submitted in relation to the online social networking service X. These decisions follow a review process conducted by the Commission after receiving the notifications of the three companies regarding their potential status as gatekeepers on 1st March 2024.
On the basis of Booking's self-assessment submitted on 1st March 2024 that it meets the relevant thresholds, the EU Commission has established that this core platform service constitutes an important gateway between businesses and consumers.
In parallel, the Commission has opened a market investigation to further assess the rebuttal submitted on 1 March 2024 in relation to the online social networking service X. This rebuttal argues that, despite

meeting the thresholds, X does not qualify as an important gateway between businesses and consumers. The investigation should be completed within five months.

---

**12 May 2024 - EU Commission launches Whistleblower Tools for Digital Services Act and Digital Markets Act.**

The European Commission has launched two whistleblower tools for the Digital Services Act (DSA) and Digital Markets Act (DMA). The tools will make it possible for individuals to provide, without fear of reprisals, information allowing to identify and uncover harmful practices of Very Large Online Platforms (VLOPs) or Search Engines (VLOSEs) designated under the Digital Services Act - DSA, or any violations of the obligations of gatekeepers under the Digital Markets Act - DMA.

Whistleblowers can provide relevant information anonymously or not, in any of the EU official language and in any relevant format (for example, reports, memos, email exchanges, data metrics, internal research, decisions or any relevant circumstances). The whistleblower tools offer a secure way to report such information. All data is encrypted, ensuring robust protection and adherence to standard legal frameworks. The tools have been certified by an independent third party, guaranteeing the complete privacy of the whistleblower in all its communications with the Commission.

Individuals who encounter harmful practices by VLOPs or VLOSEs can, under the DSA, lodge complaints with their national Digital Services Coordinator. Any instance of non-compliance with the DMA by gatekeepers can be reported to the dedicated Commission contact point or to national competition authorities of their Member State where the complainant is based. More information is available at the Commission's whistleblower tools website for DSA and DMA.

---

## INFORMATION TECHNOLOGY

**6 May 2024 - Supreme Court of Cassation: certified electronic mail (PEC) is suitable for proving the sending and receipt of a message, but not for guaranteeing the content of the document attached to it.**

Certified electronic mail (PEC) certifies the origin of the message, and the date of sending, but from this it is not possible to ascertain that the attached document is also referable to its author and that it actually has that content. Therefore, certified electronic mail (CEM) is able to certify with certainty the transmission and receipt of the message, the method of dispatch (date, time and format) and also its content, but limited to the CEM itself, not to the file attached to it.
If a file with a certain name, extension, format and size has been attached to the PEC, the receipt will attest to this, but will not be proof of the content of that file, requiring, for this purpose, a digital signature to be affixed to the attached file, which will certify the origin of the document and its integrity.
The production of the certified electronic mail in electronic format is therefore not capable of providing proof of the content of the attached document (and of its date certainty). Likewise, the certainty of the date of the CEM does not extend to the private contract referred to therein.

---